EXHIBIT A

Supreme Court of Pennsylvania

Court of Common Pleas
Civil Cover Sheet

Cumberland **County**

For Prothonotary Use Only:	TIME STAMP
Docket No: 2024-02374	

The information collected on this form is used solely for court administration purposes. This form does not supplement or replace the filing and service of pleadings or other papers as required by law or rules of court.

Commencement of Action:
☒ Complaint ☐ Writ of Summons ☐ Petition
☐ Transfer from Another Jurisdiction ☐ Declaration of Taking

Lead Plaintiff's Name:	Lead Defendant's Name:
John Doe	Post Acute Medical, LLC d/b/a PAM Health
Are money damages requested? ☒ Yes ☐ No	Dollar Amount Requested: (check one) ☐ within arbitration limits ☒ outside arbitration limits
Is this a *Class Action Suit*? ☒ Yes ☐ No	**Is this an *MDJ Appeal*?** ☐ Yes ☒ No

Name of Plaintiff/Appellant's Attorney: Patrick Howard

☐ **Check here if you have no attorney (are a Self-Represented [Pro Se] Litigant)**

Nature of the Case: Place an "X" to the left of the **ONE** case category that most accurately describes your ***PRIMARY CASE.*** If you are making more than one type of claim, check the one that you consider most important.

TORT (*do not include Mass Tort*)
- ☐ Intentional
- ☐ Malicious Prosecution
- ☐ Motor Vehicle
- ☐ Nuisance
- ☐ Premises Liability
- ☐ Product Liability *(does not include mass tort)*
- ☐ Slander/Libel/ Defamation
- ☐ Other:

MASS TORT
- ☐ Asbestos
- ☐ Tobacco
- ☐ Toxic Tort - DES
- ☐ Toxic Tort - Implant
- ☐ Toxic Waste
- ☐ Other:

PROFESSIONAL LIABLITY
- ☐ Dental
- ☐ Legal
- ☐ Medical
- ☐ Other Professional:

CONTRACT (*do not include Judgments*)
- ☐ Buyer Plaintiff
- ☐ Debt Collection: Credit Card
- ☐ Debt Collection: Other
- ☐ Employment Dispute: Discrimination
- ☐ Employment Dispute: Other
- ☐ Other:

REAL PROPERTY
- ☐ Ejectment
- ☐ Eminent Domain/Condemnation
- ☐ Ground Rent
- ☐ Landlord/Tenant Dispute
- ☐ Mortgage Foreclosure: Residential
- ☐ Mortgage Foreclosure: Commercial
- ☐ Partition
- ☐ Quiet Title
- ☐ Other:

CIVIL APPEALS
Administrative Agencies
- ☐ Board of Assessment
- ☐ Board of Elections
- ☐ Dept. of Transportation
- ☐ Statutory Appeal: Other
- ☐ Zoning Board
- ☐ Other:

MISCELLANEOUS
- ☐ Common Law/Statutory Arbitration
- ☐ Declaratory Judgment
- ☐ Mandamus
- ☐ Non-Domestic Relations Restraining Order
- ☐ Quo Warranto
- ☐ Replevin
- ☒ Other: Improper practice of personal identifying information

Updated 1/1/2011

John Doe, et al Plaintiff	:	IN THE COURT OF COMMON PLEAS OF CUMBERLAND COUNTY, PENNSYLVANIA
Post Acute Medical, LLC d/b/a PAM Health and PAM Health, LLC Defendant	:	NO. _____ 20 24 Civil Term

NOTICE TO DEFEND

YOU HAVE BEEN SUED IN COURT. IF YOU WISH TO DEFEND AGAINST THE CLAIMS SET FORTH IN THE FOLLOWING PAGES, YOU MUST TAKE ACTION WITHIN TWENTY (20) DAYS AFTER THIS COMPLAINT AND NOTICE ARE SERVED, BY ENTERING A WRITTEN APPEARANCE PERSONALLY OR BY AN ATTORNEY AND FILLING IN WRITING WITH THE COURT YOUR DEFENSES OR OBJECTIONS TO THE CLAIMS SET FORTH AGAINST YOU. YOU ARE WARNED THAT IF YOU FAIL TO DO SO THE CASE MAY PROCEED WITHOUT YOU AND A JUDGEMENT MAY BE ENTERED AGAINST YOU BY THE COURT WITHOUT FURTHER NOTICE FOR ANY MONEY CLAIMED IN THE COMPLAINT OR FOR ANY OTHER CLAIM OR RELIEF REQUESTED BY THE PLAINTIFF. YOU MAY LOSE MONEY OR PEOPERTY OR OTHER RIGHTS IMPORTANT TO YOU.

YOU SHOULD TAKE THIS PAPER TO YOUR LAWYER AT ONCE. IF YOU DO NOT HAVE A LAWYER OR CANNOT AFFORD ONE, GO TO THE TELEPHONE OR THE OFFICE SET FORTH BELOW TO FIND WHERE YOU CAN GET LEGAL HELP.

CUMBERLAND COUNTY BAR ASSOCIATION
32 SOUTH BEDFORD STREET
CARLISLE, PA 17013
1-800-990-9108
717-249-3166

TRUE COPY FROM RECORD
In Testimony whereof, I here unto set my hand and the seal of said Court at Carlisle, Pa.
This 8 day of MARCH, 20 24
Prothonotary
DPTY

SALTZ MONGELUZZI & BENDESKY P.C.
BY: PATRICK HOWARD (PA Atty ID #88572)
ONE LIBERTY PLACE, 52ND FLOOR
1650 MARKET STREET
PHILADELPHIA, PA 19103
(215) 496-8282

COHEN & MALAD, LLP
BY: LYNN TOOPS/MARY KATE DUGAN
PRO HAC VICE PENDING
ONE INDIANA SQUARE, SUITE 1400
INDIANAPOLIS, IN 46204
(317) 636-6481

TURKE & STRAUSS LLP
BY: RAINA C. BORRELLI/SAMUEL J. STRAUSS
PRO HAC VICE PENDING
613 WILLIAMSON STREET, SUITE 201
MADISON, WI 53703
(608) 237-1775

STRANCH, JENNINGS & GARVEY, PLLC
J. GERARD STRANCH, IV/ANDREW E. MIZE
PRO HAC VICE PENDING
223 ROSA L. PARKS AVENUE, SUITE 200
NASHVILLE, TN 37203
(615) 254-8801

Attorneys for Plaintiff

CUMBERLAND COUNTY COURT OF COMMON PLEAS

JOHN DOE, Individually, as Personal Representative of the Estate of JANE DOE, and on behalf of all others similarly situated,	)	
Plaintiff	)	**Case No.** _____
v.	)	
POST ACUTE MEDICAL, LLC D/B/A PAM HEALTH, and PAM HEALTH, LLC	)	JURY TRIAL DEMANDED
Defendants.	)	

CLASS ACTION COMPLAINT

Plaintiff, JOHN DOE, Individually, as Personal Representative of the Estate of JANE DOE (hereinafter, "Plaintiff"), and on behalf of all others similarly situated, brings this Class Action Complaint against Defendants, POST ACUTE MEDICAL, LLC D/B/A PAM HEALTH, and PAM HEALTH, LLC (hereinafter, collectively, "PAM Health" or "Defendants"), and alleges, upon personal knowledge as to his own actions, and upon information and belief as to all other matters, as follows.

INTRODUCTION

1. Plaintiff brings this class action to address Defendants' improper practice of disclosing the confidential Personally Identifying Information ("PII")[1] and/or Protected Health Information ("PHI")[2] (collectively referred to as "Private Information") of Plaintiff and the proposed Class Members to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook" or "Meta"),[3] Google, LLC ("Google"), Microsoft, MarketingCloudFX, and potentially others via tracking technologies used on its website ("the Disclosure").

---

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 16, 2020). PAM Health is clearly a "covered entity" and some of the data compromised in the Disclosure that this action arises out of is "protected health information," subject to HIPAA.

[3] Facebook changed its name from Facebook, Inc. to Meta Platforms, Inc. in October 2021. Plaintiff's reference to both "Facebook" and "Meta" throughout this complaint refer to the same company.

2. The Office for Civil Rights ("OCR") at the U.S. Department of Health and Human Services ("HHS") and the Federal Trade Commission ("FTC") warn about the "serious privacy and security risks related to the use of online tracking technologies" present on websites or online platforms, such as Defendants', that "impermissibly disclos[e] consumers' sensitive personal health information to third parties."[4] OCR and FTC agree that such tracking technologies, like those present on Defendants' website, "can track a user's online activities" and "gather identifiable information about users as they interact with a website or mobile app, often in ways which are not avoidable by and largely unknown to users."[5] OCR and FTC warn that "[i]mpermissible disclosures of an individual's personal health information to third parties may result in a wide range of harms to an individual or others. Such disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more. In addition, impermissible disclosures of personal health information may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others."[6]

3. Information about a person's physical and mental health is among the most confidential and sensitive information in our society, and the mishandling of medical information can have serious consequences, including discrimination in the workplace or denial of insurance coverage. If people do not trust that their medical information will be kept private, they may be less likely to seek medical treatment, which can lead to more serious health problems down the

[4] Re: Use of Online Tracking Technologies, U.S. Dep't of Health & Human Services (July 20, 2023), available at https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf, **attached as Exhibit A.**

[5] *Id.*

[6] Re: Use of Online Tracking Technologies, **Exhibit A.**

road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to anyone other than the person's medical provider is necessary to maintain public trust in the healthcare system as a whole.

4. Recognizing these facts, and in order to implement requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), HHS has established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") governing how health care providers must safeguard and protect Private Information. Under the HIPAA Privacy Rule, no health care provider can disclose a person's personally identifiable protected health information to a third party without express written authorization.

5. Headquartered in Pennsylvania, PAM Health is a massive healthcare system which provides treatment to patients in Pennsylvania, Ohio, and across the country under a mission of "…providing high-quality patient care and outstanding customer service, coupled with loyal, dedicated, and highly trained staff, to be the most trusted and impactful source for healthcare services in every community it serves."[7]

6. Despite its unique position as a massive and trusted healthcare provider, PAM Health knowingly configured and implemented into its website, https://pamhealth.com/ (the "Website") code-based tracking devices known as "pixels" (also referred to as "trackers" or "tracking technologies"), which collected and transmitted patients' Private Information to Facebook and other third parties, without patients' knowledge or authorization.

7. Defendants encourages patients to use their Website, along with their various web-based tools and services (collectively, the "Online Platforms"), to learn about PAM Health on its

[7] https://pamhealth.com/company/about-us (last acc. March 6, 2024).

main homepage,[8] to search for health information, medical conditions, and physicians;[9] to find locations,[10] to research particular facilities,[11] to research medical treatments and conditions,[12] and more such as to make payments,[13] to find out pertinent information on health topics via Defendants' blog,[14] and to access a patient portal.[15]

8. When Plaintiff and Class Members used Defendants' Website and Online Platforms, they thought they were communicating exclusively with their trusted healthcare provider. Unbeknownst to them, Defendants embedded pixels from Facebook, Google, and likely others into its Website and Online Platforms, surreptitiously forcing Plaintiff and Class Members to transmit intimate details about their medical treatment to third parties without their consent.

9. A pixel (also referred to as a "tracker" or "tracking technology") is a snippet of code embedded into a website that tracks information about its visitors and their website interactions.[16] When a person visits a website with an embedded pixel, the pixel tracks "events" (i.e., user interactions with the site), such as pages viewed, buttons clicked, and information submitted.[17] Then, the pixel transmits the event information back to the website server and to third parties, where it can be combined with other data and used for marketing.[18]

10. Among the trackers Defendants embedded into its Website is the Facebook Pixel

---

[8] https://pamhealth.com/ (last acc. Mar. 6, 2024).
[9] E.g., search for "amputation" avail. at https://pamhealth.com/search-results?search_paths%5B%5D=&query=amputation (last acc. Mar. 6, 2024).
[10] https://pamhealth.com/facilities (last acc. Mar. 6, 2024).
[11] E.g., rehabilitation hospitals, avail. at https://pamhealth.com/facilities/find-facility/rehabilitation-hospitals (last acc. Mar. 6, 2024).
[12] https://pamhealth.com/health-services (last acc. Mar. 6, 2024).
[13] https://post.patientbillhelp.com/ (last acc. Mar. 6, 2024).
[14] https://pamhealth.com/company/company-updates (last acc. Mar. 6, 2024).
[15] https://pamhealth.com/login (last acc. Mar. 6, 2024).
[16] *See* Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).
[17] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited May 22, 2023).
[18] *Id.*

(also referred to as the "Meta Pixel" or "Pixel"). By default, the Meta Pixel tracks information about a visitor's device, including their IP address, and the pages viewed.[19] When configured to do so, the Meta Pixel can track much more, including a visitor's search terms, button clicks, and form submissions.[20] Additionally, the Meta Pixel can link a visitor's website interactions with an individual's unique and persistent Facebook ID ("FID"), allowing a user's health information to be linked with their Facebook profile.[21]

11. Operating as designed and as implemented by Defendants, the Meta Pixel allowed Defendants to unlawfully disclose Plaintiff and Class Members' Private Health Information alongside identifying details to Facebook. By installing the Meta Pixel on its Website, Defendants effectively planted a bug on Plaintiff's and Class Members' web browsers and compelled them to disclose Private Information and confidential communications to Facebook without their authorization or knowledge.

12. Facebook encourages and recommends use of its Conversions Application Programming Interface ("CAPI") alongside use of the Meta Pixel.[22]

13. Unlike the Meta Pixel, which co-opts a website user's browser and forces it to

---

[19] *See* Get Started, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/get-started (last visited May 22, 2023).

[20] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited May 22, 2023).

[21] The Meta Pixel forces the website user to share the user's FID for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the same web browser. "Cookies are small files of information that a web server generates and sends to a web browser." "Cookies help inform websites about the user, enabling the websites to personalize the user experience." What are Cookies?, https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Jan. 27, 2023).

[22] "CAPI works with your Meta Pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* Samir El Kamouny, How to Implement Facebook Conversions API (In Shopify), FETCH & FUNNEL https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited Jan. 25, 2023).

transmit information to Facebook in addition to the website owner, CAPI does not cause the user's browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website interaction, including Private Information, records and stores that information on the website owner's servers, and then transmits the data to Facebook from the website owner's servers.[23, 24]

14. Indeed, Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[25]

15. Because CAPI is located on the website owner's servers and is not a bug planted onto the website user's browser, it allows website owners like Defendants to circumvent any ad blockers or other denials of consent by the website user that would prevent the Meta Pixel from sending website users' Private Information to Facebook directly.

16. Defendants utilized data from these trackers to market its services and bolster its profits. Meta Pixel and CAPI are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting and future marketing. Facebook also uses Plaintiff's and Class Members' Private Information to create targeted advertisements based on the medical conditions and other information disclosed to Defendants.

17. The information that Defendants' Meta Pixel and possibly CAPI sent to Facebook can include the Private Information that Plaintiff and Class Members submitted to Defendants'

---

[23] What is the Facebook Conversion API and How to Use It, REVEALBOT BLOG, https://revealbot.com/blog/facebook-conversions-api/ (last updated May 20, 2022).

[24] "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel.... This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels." Conversions API, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/conversions-api (last visited May 15, 2023).

[25] About Conversions API, META FOR DEVELOPERS, https://www.facebook.com/business/help/2041148702652965 (last visited May 15, 2023).

Website, including details about the pages they browsed and the buttons they clicked, their search terms, the locations and facilities they viewed, the medical treatment services they browsed, the conditions they researched, as well as information about their identities.

18. Such information allows a third party (e.g., Facebook) to know that a specific patient was seeking confidential medical care. Facebook, in turn, sells Plaintiff's and Class Members' Private Information to third-party marketers, who then geotarget Plaintiff's and Class Members' Facebook pages based on communications obtained via the Meta Pixel and CAPI. Facebook and any third-party purchasers of Plaintiff's and Class Members' Private Information also could reasonably infer from the data that a specific patient was being treated for a specific type of medical condition, such as cancer, pregnancy, dementia, or HIV.

19. In addition to the Facebook tracker and CAPI, on information and belief, Defendants installed other tracking technology which operate similarly to the Meta Pixel and transmit a website user's Private Information to other third parties.

20. Healthcare patients simply do not anticipate that their trusted healthcare provider will send Personal Health Information ("PHI") or other confidential medical information collected via its webpages to a hidden third party—let alone Facebook, which has a sordid history of privacy violations in pursuit of ever-increasing advertising revenue—without the patients' consent.

21. Neither Plaintiff nor any Class Member signed a written authorization permitting Defendants to send their Private Information to Facebook, or any other third parties uninvolved in their treatment.

22. Despite willfully and intentionally incorporating tracking technology, including the Meta Pixel, potentially CAPI, and other tracking technology, into its Website and servers, PAM Health has never disclosed to Plaintiff or Class Members that it shared their sensitive and

confidential communications and Private Information with third parties including Facebook, Google, Microsoft, MarketingCloudFX, and potentially others.

23. Defendants further made express and implied promises to protect Plaintiff's and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchanged with Defendants, including in its privacy policies and elsewhere.

24. Defendants owed common law, statutory, and regulatory duties to keep Plaintiff's and Class Members' communications and Private Information safe, secure, and confidential.

25. Upon information and belief, PAM Health utilized the Meta Pixel and other tracker data to improve and to save costs on its marketing campaigns, improve its data analytics, attract new patients, and generate sales.

26. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendants assumed legal and equitable duties to those individuals to protect and to safeguard that information from unauthorized disclosure.

27. Defendants breached their statutory and common law obligations to Plaintiff and Class Members by, *inter alia*,: (i) failing to adequately review its marketing programs and web based technology to ensure the hospital Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) aiding, agreeing, and conspiring with third parties to intercept communications sent and received by Plaintiff and Class Members; (iv) failing to obtain the written consent of Plaintiff and Class Members to disclose their Private Information to Facebook and others; (v) failing to protect Private Information and take steps to block the transmission of Plaintiff's and Class Members' Private Information through the use of Meta Pixel and other tracking technology; (vi) failing to warn

Plaintiff and Class Members; and (vii) otherwise failing to design and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

28. Plaintiff seeks to remedy these harms and brings causes of action for (I) Negligence, (II) Invasion of Privacy—Intrusion Upon Seclusion; (III) Invasion of Privacy—Public Disclosure of Private Facts; (IV) Breach of Implied Contract; (V) Unjust Enrichment; (VI) Breach of Fiduciary Duty; (VII) violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 Pa. Stat. § 20101, *et seq.* ("UTPCPL"); and (VIII) violation of the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. C.S. § 5701, *et seq.*, ("WESCA").

PARTIES

29. Plaintiff, JOHN DOE, is a natural person and a resident and citizen of the State of Ohio where he intends to remain, with a principal residence in Batavia, Ohio, in Clermont County. Plaintiff is the Personal Representative for the Estate of his late wife, JANE DOE.

30. Defendants, POST ACUTE MEDICAL, LLC D/B/A PAM HEALTH is a limited liability company organized and existing under the laws of the State of Delaware with its principal place of business in the Commonwealth of Pennsylvania at 1828 Good Hope Road, Suite 102, Enola, Pennsylvania 17025, in Cumberland County.

31. Defendants, PAM HEALTH, LLC, is a limited liability company organized and existing under the laws of the Commonwealth of Pennsylvania with its principal place of business at 1828 Good Hope Road, Suite 102, Enola, Pennsylvania 17025 in Cumberland County.

JURISDICTION & VENUE

32. This Court has jurisdiction over the subject matter of this action pursuant to 42 Pa. Cons. Stat. § 931.

33. This Court has personal jurisdiction over Defendants pursuant to 42 Pa. Cons.

Stat. § 5301, because Defendants each carry on a continuous and systematic part of their general business within this Commonwealth and maintain principal places of business herein.

34. Venue is appropriate in this Court under 231 Pa. Code § 2179, because Defendants' principal places of business are in Cumberland County.

COMMON FACTUAL ALLEGATIONS

A. Background

35. Founded in 2006 and headquartered in Enola, Pennsylvania, PAM Health is a massive, national medical system which owns and operates medical facilities in Ohio, Pennsylvania, Kentucky, Missouri, North Carolina, Florida, Louisiana, Texas, Arizona, Nevada, Colorado, and North Dakota.[26]

36. PAM Health generates approximately $890 million in annual revenue, and employs 7,500 people.[27]

37. Defendants provide medical services at numerous rehabilitation hospitals, specialty hospitals, outpatient centers, and behavioral health hospitals, and provide home health and hospice services.[28]

38. At these locations, PAM Health provides medical services in numerous departments and programs, including for amputations, brain injuries, cardio/pulmonary, diabetes, Fibromyalgia/Rheumatoid conditions, fractures, Guillian-Barre Syndrome, hip/knee replacements, infections, Lymphedema, Multiple Sclerosis, Neurological conditions, oncology, osteoarthritis, osteoporosis, Parkinson's, Peripheral Vascular Disease, Renal conditions, respiratory failure, spinal cord injury, stroke (CVA), and for wounds.[29]

---

[26] *See generally* https://pamhealth.com/facilities (last acc. Mar. 6, 2024).
[27] https://www.zippia.com/post-acute-medical-careers-35227/revenue/ (last acc. Mar. 6, 2024).
[28] *See generally* https://pamhealth.com/facilities (last acc. Mar. 6, 2024).
[29] *Id.*

39. Further, PAM Health provides Physical Therapy, Occupational Therapy, Speech Therapy, and Nursing Services (including IV Therapy, Central Line and PICC Line, Telemetry Monitoring, Hemodynamic Monitoring, and Certified Wound Care Nurses) as well as behavioral health treatment in conjunction with Voyages Behavioral Health.[30]

40. PAM Health provides outpatient rehabilitation services at numerous clinics, *to wit*:

- PAM Health Rehabilitation Hospital of Surprise, Surprise, Arizona;
- PAM Health Rehabilitation Hospital of Westminster, Westminster, Colorado;
- PAM Health Rehabilitation Hospital of Greeley (coming soon), Greeley, Colorado;
- PAM Health Rehabilitation Hospital of Dover, Dover, Delaware;
- PAM Health Rehabilitation Hospital of Georgetown, Georgetown, Delaware;
- PAM Health Specialty Hospital of Jacksonville, Jacksonville, Florida;
- PAM Health Rehabilitation Hospital of Jupiter, Jupiter, Florida;
- PAM Health Rehabilitation Hospital of Tavares, Tavares, Florida;
- PAM Health Rehabilitation Hospital of Venice (coming soon), Nokomis, Florida;
- PAM Health Rehabilitation Hospital of Greater Indiana, Clarksville, Indiana;
- PAM Health Rehabilitation Hospital of Overland Park, Overland Park, Kansas;
- PAM Health Rehabilitation Hospital of Centennial Hills, Las Vegas, Nevada;
- PAM Health Rehabilitation Hospital of Fargo, Fargo, North Dakota;
- PAM Health Rehabilitation Hospital of Miamisburg, Miamisburg, Ohio;
- PAM Health Rehabilitation Hospital of Tulsa, Tulsa, Oklahoma;
- PAM Health Rehabilitation Hospital of Allen: Outpatient Therapy, Allen, Texas;
- PAM Health Rehabilitation Hospital of Beaumont, Beaumont, Texas;
- PAM Health Rehabilitation Hospital of Clear Lake, Webster, Texas;
- PAM Health Rehabilitation Hospital of Clear Lake North, Webster, Texas
- PAM Health Rehabilitation Hospital of Corpus Christi, Corpus Christi, Texas;
- PAM Health Rehabilitation Hospital of El Paso, El Paso, Texas;
- PAM Health Rehabilitation Hospital of Humble, Humble, Texas;
- PAM Health Rehabilitation Hospital of Kyle, Kyle, Texas;
- PAM Health Rehabilitation Clinic of Lockhart, Lockhart, Texas;
- PAM Health Specialty Hospital of Luling, Luling, Texas;
- PAM Health Rehabilitation Hospital of Round Rock, Round Rock, Texas;
- PAM Health Warm Springs Rehabilitation Hospital of San Antonio, San

[30] https://pamhealth.com/health-services (last acc. Mar. 6, 2024).

Antonio, Texas;
- PAM Health Rehabilitation Hospital of Sugar Land, Sugar Land, Texas;
- PAM Health Hospital of Victoria North, Victoria, Texas; and
- PAM Health Warm Springs Rehabilitation Hospital of Westover Hills, San Antonio, Texas.[31]

41. One of Defendants' rehabilitation facilities is PAM Health Specialty Hospital of Dayton, a "long-term acute care hospital in Dayton, OH, specializing in the treatment of medically complex patients who require extended hospitalization" with "44 licensed beds and a medical staff of more than 125 physicians."[32]

42. PAM Health Specialty Hospital of Dayton provides Long-term acute care (LTACH) ("complex medical management, therapeutic care and rehabilitation services -- 24 hours a day, 7 days a week, with daily assessment of the patient by a physician"), including " Core Specialty Programs" including Pulmonary – Ventilator Weaning/Trach Care, Medically Complex, Advanced Wound Care Program, Rehabilitation Advanced Respiratory Therapy Modalities, Early Mobility Program and, a Nutritional Program; and specialty services and treatment such as Hemodialysis/Peritoneal Dialysis, Pulmonary Services, Vent Weaning, Telemetry Monitoring, Complex Wounds, Infectious Diseases, Multiple Intravenous Therapies, Post - OP Complications, TPN and other Nutritional Interventions, Catastrophic Injuries, Pain Management, On-Site Pharmacy, Vital Stim, and Bariatric.[33]

43. Defendants tout PAM Health's "We Care" program towards the goal of ensuring effective communication with patients and their families:

> …to make sure that we are providing the very best care for our patients. We strive to ensure that our patients feel valued, and that they are receiving the very best clinical and emotional support possible. We encourage our patients and their families to be involved in their treatment plan from admission to post-discharge

[31] https://pamhealth.com/facilities/find-facility/outpatient-centers (last acc. Mar. 6, 2024).
[32] https://pamhealth.com/facilities/find-facility/specialty-hospitals/PAM-Specialty-Hospital-of-Dayton (last acc. Mar. 6, 2024).
[33] *Id.*

and it is our goal to educate them for success in their recovery.[34]

44. The "We Care" program includes assigning each patient a "patient partner" who has the "responsibility to keep the patient and their family informed throughout their stay and make sure that we are meeting all of their expectations," and who follows-up with patients following discharge.[35]

45. PAM Health serves many of its patients via its Online Platforms, which it encourages patients, to use to learn about PAM Health on its main homepage,[36] to search for health information, medical conditions, and physicians;[37] to find locations,[38] to research particular facilities,[39] to research medical treatments and conditions,[40] and more such as to make payments,[41] to find out pertinent information on health topics via Defendants' blog,[42] and to access a patient portal.[43]

46. In furtherance of its goal of increasing sales and profitability, and to improve the success of its advertising and marketing, Defendants purposely installed the Meta Pixel and other trackers onto its Website, for the purpose of gathering information about Plaintiff and Class Members to further its marketing efforts. But Defendants did not only generate information for its own use: it also shared patient information, including Private Information belonging to Plaintiff and Class Members, with Facebook and other unauthorized third parties.

---

[34] https://pamhealth.com/health-services/we-care (last acc. Mar. 6, 2024).
[35] *Id.*
[36] https://pamhealth.com/ (last acc. Mar. 6, 2024).
[37] E.g., search for "amputation" avail. at https://pamhealth.com/search-results?search_paths%5B%5D=&query=amputation (last acc. Mar. 6, 2024).
[38] https://pamhealth.com/facilities (last acc. Mar. 6, 2024).
[39] E.g., rehabilitation hospitals, avail. at https://pamhealth.com/facilities/find-facility/rehabilitation-hospitals (last acc. Mar. 6, 2024).
[40] https://pamhealth.com/health-services (last acc. Mar. 6, 2024).
[41] https://post.patientbillhelp.com/ (last acc. Mar. 6, 2024).
[42] https://pamhealth.com/company/company-updates (last acc. Mar. 6, 2024).
[43] https://pamhealth.com/login (last acc. Mar. 6, 2024).

47. To better understand Defendants' unlawful data-sharing practices, a brief discussion of basic web design and tracking tools follows.

i. Facebook's Business Tools and the Meta Pixel

48. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[44]

49. In conjunction with its advertising business, Facebook encourages and promotes entities and website owners, such as Defendants, to utilizes its "Business Tools" to gather, identify, target, and market products and services to individuals.

50. Facebook's Business Tools, including the Meta Pixel and Conversions API, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user activity on those platforms.

51. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, the webpage's Universal Resource Locator ("URL"), as well as metadata, button clicks, and other information.[45] Businesses that want to target customers and advertise their services, such as Defendants, can track other user actions and can create their own tracking parameters by building a "custom event."[46]

52. One such Business Tool is the Meta Pixel, a tool that "tracks the people and type

---

[44] Meta Reports Fourth Quarter and Full Year 2021 Results, FACEBOOK https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Nov. 14, 2022).

[45] Specifications for Facebook Pixel Standard Events, META, https://www.facebook.com/business/help/402791146561655 (last visited Jan. 31, 2023); *see also* Facebook Pixel, Accurate Event Tracking, Advanced, META FOR DEVELOPERS; https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* Best Practices for Facebook Pixel Setup, META https://www.facebook.com/business/help/218844828315224; App Events API, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Jan. 31, 2023).

[46] About Standard and Custom Website Events, META, https://www.facebook.com/business/help/964258670337005; *see also* Facebook, App Events API, *supra*.

of actions they take."[47] When a user accesses a webpage that is hosting the Meta Pixel, the communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook—traveling from the user's browser to Facebook's server.

53. Notably, this transmission only occurs on webpages that contain the Pixel. A website owner can configure its website to use the Pixel on certain webpages that don't implicate patient privacy (such as the homepage) and disable it on pages that do implicate patient privacy (such as Defendants' "Services" pages[48]).

54. The Meta Pixel's primary purpose is for marketing and ad targeting and sales generation.[49]

55. Facebook's own website informs companies that "[t]he Meta Pixel is a piece of code that you put on your website that allows you to measure the effectiveness of your advertising by understanding the actions people take on your website."[50]

56. According to Facebook, the Meta Pixel can collect the following data.

> **Http Headers** – Anything present in HTTP headers. HTTP Headers are a standard web protocol sent between any browser request and any server on the internet. HTTP Headers include IP addresses, information about the web browser, page location, document, referrer and ***person using the website.*** (emphasis added).
>
> **Pixel-specific Data** – Includes Pixel ID and the Facebook Cookie.
>
> **Button Click Data** – Includes any buttons clicked by site visitors, the labels those buttons and any pages visited as a result of the button clicks.
>
> **Optional Values** – Developers and marketers can optionally choose to send additional information about the visit through Custom Data events. Example custom data events are conversion value, page type and more.

---

[47] Retargeting, META, https://www.facebook.com/business/goals/retargeting.
[48] https://pamhealth.com/health-services (last acc. Mar. 6, 2024).
[49] *See* Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).
[50] About Meta Pixel, META, https://www.facebook.com/business/help/742478679120153 (last accessed Mar. 19, 2023).

Form Field Names – Includes website field names like email, address, quantity, etc., for when you purchase a product or service. We don't capture field values unless you include them as part of Advanced Matching or optional values.[51]

57. Facebook boasts to its prospective users that the Meta Pixel can be used to:

- **Make sure your ads are shown to the right people.** Find new customers, or people who have visited a specific page or taken a desired action on your website.
- **Drive more sales.** Set up automatic bidding to reach people who are more likely to take an action you care about, like making a purchase.
- **Measure the results of your ads.** Better understand the impact of your ads by measuring what happens when people see them.[52]

58. Facebook likewise benefits from the data received from the Meta Pixel and uses the data to serve targeted ads and identify users to be included in such targeted ads.

ii. Defendants' method of transmitting Plaintiff's and Class Members' Private Information via the Meta Pixel and/or Conversions API i.e., the Interplay between HTTP Requests and Responses, Source Code, and the Meta Pixel

59. Web browsers are software applications that allow consumers to navigate the internet and view and exchange electronic information and communications. Each "client device" (such as computer, tablet, or smart phone) accesses web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

60. Every website is hosted by a computer "server" that holds the website's contents and through which the website owner exchanges files or communications with Internet users' client devices via their web browsers.

61. Web communications consist of HTTP Requests and HTTP Responses, and any

[51] Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).
[52] About Meta Pixel, META, https://www.facebook.com/business/help/742478679120153 (last accessed Mar. 19, 2023).

given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies.[53]

62. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), they also send the host server data, which is embedded inside the URL and can include cookies.

63. When an individual visits a website, their web browser sends an HTTP Request to the entity's servers that essentially asks the website to retrieve certain information (such as Defendants' search function page). The entity's servers send the HTTP Response, which contains the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate a website.

64. Every website is comprised of Markup and "Source Code." Source Code is simply a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

65. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user.

66. Defendants' implementation of the Meta Pixel is source code that acted much like a traditional wiretap, intercepting and transmitting communications intended only for Defendants.

67. Separate from the Meta Pixel, Facebook and other website owners can place third-party cookies in the web browsers of users logged into their websites or services. These cookies can uniquely identify the user so the cookie owner can track the user as she moves around the

[53] "Cookies are small files of information that a web server generates and sends to a web browser . . . . Cookies help inform websites about the user, enabling the websites to personalize the user experience." https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Jan. 27, 2023).

internet—whether on the cookie owner's website or not. Facebook uses this type of third-party cookie when Facebook account holders use the Facebook app or website. As a result, when a Facebook account holder uses Defendants' Website, the account holder's unique Facebook ID is sent to Facebook, along with the intercepted communication, allowing Facebook to identify the patient associated with the Private Information it has intercepted.

68. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. To counteract this, third parties bent on gathering data and Private Information implement workarounds that are difficult to detect or evade. Facebook's workaround is its Conversions API tool, which is particularly effective because the data transmitted via this tool does not rely on the website visitor's web browsers. Rather, the information travels directly from the entity's server to Facebook's server.

69. Conversions API "is designed to create a direct connection between [web hosts'] marketing data and [Facebook]."[54] Thus, the entity receives and stores its communications with patients on its server before Conversions API collects and sends those communications—and the Private Information contained therein—to Facebook.

70. Notably, client devices do not have access to host servers and thus cannot prevent (or even detect) this additional transmission of information to Facebook.

71. While there is no way to confirm with certainty that a website owner is using Conversions API without accessing the host server, Facebook instructs companies like Defendants to "[u]se the Conversions API in addition to the Meta Pixel, and share the same events using both tools," because such a "redundant event setup" allows the entity "to share website events [with

[54] About Conversions API, META, https://www.facebook.com/business/help/2041148702652965 (last visited May 15, 2023).

Facebook] that the pixel may lose."[55] Thus, if an entity implemented the Meta Pixel in accordance with Facebook's documentation, it is also reasonable to infer that it implemented the Conversions API tool on its Website.

72. The third parties to whom a website transmits data through pixels and other tracking technology do not provide any substantive content on the host website. In other words, Facebook and others like it are not providing anything to the user relating to the user's communications. Instead, these third parties are typically procured to track user data and communications only to serve the marketing purposes of the website owner (i.e., to bolster profits).

73. Accordingly, without any knowledge, authorization, or action by a user, a website owner like Defendants can use its source code to commandeer its patients' computing devices, causing the device's web browser to contemporaneously and invisibly re-direct the patients' communications to hidden third parties like Facebook.

74. In this case, Defendants employed the Meta Pixel and potentially Conversions API to intercept, duplicate, and re-direct Plaintiff's and Class Members' Private Information to Facebook contemporaneously, invisibly, and without the patient's knowledge.

75. Consequently, when Plaintiff and Class Members visited Defendants' Website and communicated their Private Information, it was simultaneously intercepted and transmitted to Facebook.

76. PAM Health also employed other trackers, MarketingCloudFX, Google Analytics with Google Tag Manager ("GTM"), Facebook Events, Microsoft Clarity, and DoubleClick, which, on information and belief, likewise transmitted Plaintiff's and the Class Members' Private Information to third parties without Plaintiff's and Class Members' knowledge or authorization.

---

[55] *See* Best Practices for Conversions API, META, https://www.facebook.com/business/help/308855623839366 (last visited May 15, 2023).

iii. Defendants Violated Their own Privacy Policies

77. PAM Health maintains and is covered under privacy policies, including a Notice of Privacy Practices,[56] and a website Terms of Use Policy,[57] which are posted on Defendants' Website (collectively "Privacy Policies").

78. Defendants' Notice of Privacy Practices is applicable to:

> ...Post Acute Medical, LLC and each of its subsidiaries, affiliates, and entities managed or controlled by Post Acute Medical, including the corporate office and its employees. All of the entities will share personal health information of patients as necessary to carry out treatment, payment, and health care operations as permitted by law. **Use or disclosure pursuant to this Notice may include electronic transmittal or disclosure of your personal health information.**[58]

79. In their Notice of Privacy Practices, PAM Health states, "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."[59]

80. Therein, PAM Health represents, acknowledges, and promises:

> **We are legally required to protect the privacy of your health information.** We call this information protected health information, or PHI for short and it includes information that can be used to identify you that we have created or received about your past, present, or future health or condition, the provision of health care to you, or the payment of this health care. We must provide you with this notice about our privacy practices that explains how, when, and why we use and disclose your PHI. With some exceptions, we may not use or disclose any more of your PHI than is necessary to accomplish the purpose of the use or disclosure. We are legally required to follow the privacy practices that are described in this notice as long as it remains in effect.[60]

---

[56] Post Acute Medical, LLC, *Notice of Privacy Practices*, effective September 13, 2013, available at https://pamhealth.com/application/files/9215/3417/6221/compliance.pdf (last acc. Mar. 6, 2024), **attached as Exhibit B.**
[57] Post Acute Medical, LLC, *Terms of Use*, avail. at https://pamhealth.com/footer/terms-use (last acc. Mar. 6, 2024) **attached as Exhibit C.**
[58] Post Acute Medical, LLC, *Notice of Privacy Practices*, **Exhibit B** (bold emphasis added).
[59] *Id.* (capitalization in original)
[60] *Id.*

81. In the Notice of Privacy Practices, PAM Health further specifically represents and promises that "[w]e will not use or disclose your PHI for any purpose other than treatment, payment and healthcare operations, unless you have a signed form authorizing the use or disclosure, with exception to the situations outlined below."[61]

82. As stated in the Notice of Privacy Practices, those purposes for which Defendants may disclose Private Information/PHI without authorization further include in patient directories, to family and friends involved in patient care, and for disaster relief, as well as in connection with:

- Public health activities
- Health oversight activities
- Purposes of organ donation
- Research
- To avoid harm
- Specific government functions
- When required by federal, state or local law, judicial or administrative proceedings or law enforcement.
- Workers' Compensation
- Fundraising
- Business Associates
- Data breach notification
- Future communications
- Inmates or individuals in custody
- Appointment reminders and health related benefits or services.

[62]

83. None of the above purposes enumerated in PAM Health's Notice of Privacy Practices permit Defendants to disclose patients' PHI/Private Information to third-parties uninvolved in their treatment for marketing purposes, without their written authorization.

84. Further still, in the Notice of Privacy Practices, Defendants promise, "[i]n the event of any breach of unsecured PHI, we will comply with the HIPAA/HITECH breach notification requirements, which will include notification to you."[63]

85. In addition, Defendants maintain website Terms of Use Policy, which PAM Health informs Website users that "**By accessing and using this website, you agree to these terms and**

---

[61] *Id.*
[62] *Id.*
[63] *Id.*

conditions. PAM Health [] can change this agreement at any time. Any such modification will be effective immediately upon posting."[64]

86. Defendants' Terms of Use fail to notify Website users and patients that PAM Health utilizes the Meta Pixel and other tracking technologies to disclose PHI/Private Information to third parties such as Facebook for marketing purposes without their consent.

87. Despite these express, specific representations and promises, PAM Health does indeed transfer Private Information to third parties. Using the Meta Pixel, Defendants used and disclosed Plaintiff's and Class Member's Private Information and confidential communications to Facebook, and other unauthorized third parties, without written authorization, in violation of their Privacy Policies.

iv. PAM Health Unauthorizedly Disclosed Plaintiff's and the Class's Private Information

88. Defendants disclosed Plaintiff's and Class Members' Private Information and confidential communications to third parties for marketing purposes, including Facebook, Google, MarketingCloudFX, and Microsoft.

89. Through their use of the Meta Pixel, at least as early as December 2020, PAM Health disclosed to Facebook Plaintiff's and Class Members' Private Information communicated via its Website, including details about the pages they browsed and the buttons they clicked, their search terms, the locations and facilities they viewed, the medical treatment services they browsed, and the medical conditions they researched.

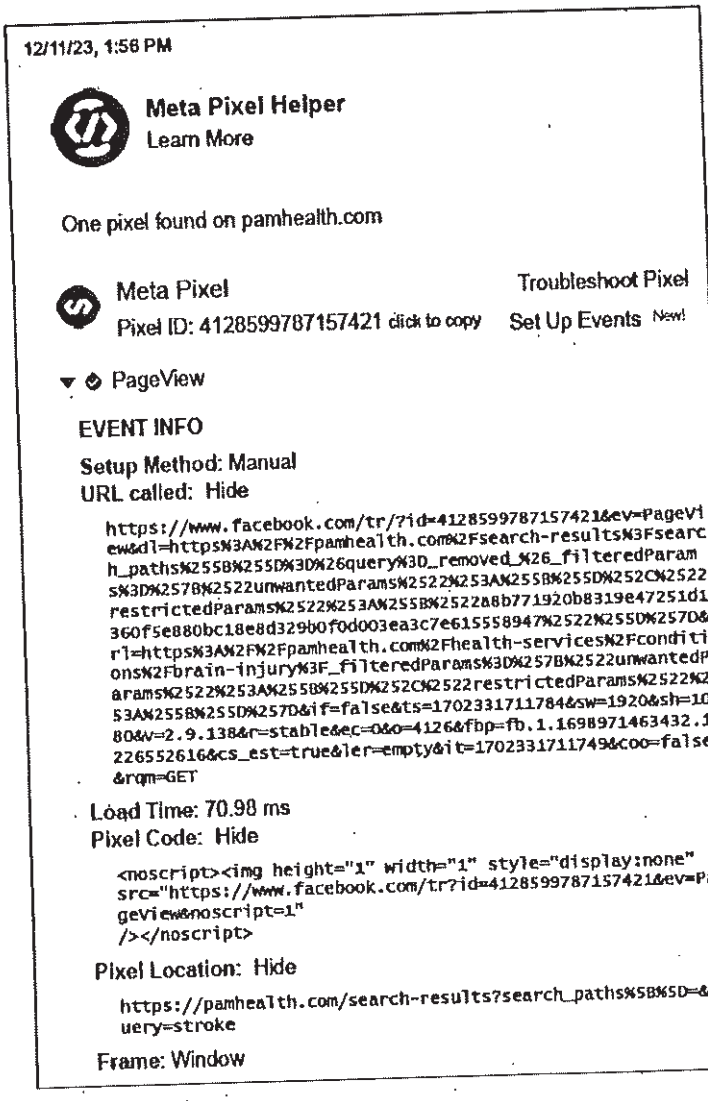
90. In addition to this information, the Meta Pixel collects and transmits to Facebook other identifying information, including IP addresses, and users' "c_user" cookies, which Facebook uses to identify users, and are transmitted in Meta Pixel events. Therefore, the Meta

[64] Post Acute Medical, LLC, *Terms of Use*, **Exhibit C** (emphasis in original)

Pixel events PAM Health sent likely allowed Facebook to connect users' identities with the details reported within the events.

91. Beginning in December 2020, and as of December 2023, Defendants utilized the Meta Pixel (ID 4128599787157421) on their Online Platforms, with Facebook Events.

92. For example, PAM Health installed the Meta Pixel on its search query page functions, e.g., for "stroke:"



93. Defendants also utilized other trackers, MarketingCloudFX, Google Analytics with Google Tag Manager ("GTM"), Facebook Events, Microsoft Clarity, and DoubleClick.

94. Of special note, the Microsoft Clarity tracker has a function enabling clients to "[e]xperience what . . . users see."[65] For example, Microsoft Clarity clients can use the tracker to replay hi-def videos of how users navigate the website and share these videos. Among its other functions, Microsoft Clarity also allows its clients to filter videos by parameters such as user location, browser, and session duration.[66]

PAM Health's Tracking and Disclosures of Users' Activities Through the Meta Pixel

95. As users navigate PAM Health's website, PAM Health transmits PageView, FindLocation, and SubscribedButtonClick events disclosing information about user activities.

96. For each of the events, PAM Health includes the "c_user" cookie, which Facebook uses to identify users.

97. PAM Health reveals users' browsing details, path of navigation throughout PAM Health's website, and interactions with elements of PAM Health's website through the events it sends to Facebook.

98. PAM Health begins its disclosures about users as soon as they arrive on PAM Health's homepage. For example, when a user loads PAM Health's homepage, PAM Health sends a PageView event, which reveals that the user is on the page, "https://pamhealth.com/."

PAM Health's Tracking and Disclosures of Users' Search Activities Via the Meta Pixel

99. PAM Health continues to report user information to Facebook as users conduct keyword searches on the website. For instance, when a user loads the results page for their search for "amputation," PAM Health sends a PageView event, disclosing that the user conducted a search and is viewing "search-results."

100. Next, as the user loads a page about PAM Health's Rehabilitation Hospital of Allen

---

[65] https://clarity.microsoft.com/session-recordings (last acc. Mar. 6, 2024).
[66] *Id.*

from the search results page, PAM Health sends another PageView event. The PageView event reveals that the user is browsing a page about "rehabilitation-hospitals/pam-rehabilitation-hospital-allen" after viewing a search results page.

101. Then, when the user clicks a button to get directions to the Allen Rehabilitation Hospital, PAM Health sends a FindLocation event, informing Facebook about that activity. The FindLocation event also divulges that the user searched for the "query=amputation," and then opened a page about the "pam-rehabilitation-hosptial-allen."

PAM Health's Tracking and Disclosures of Users' Searches for Locations Via the Meta Pixel

102. Not only does PAM Health transmit events with details about users' keyword search activities, but PAM Health also discloses when users search for PAM Health locations.

103. When a user loads a page to view PAM Health's facility locations, PAM Health sends a PageView event, revealing that the user is on the page, "https://pamhealth.com/facilities."

104. As the user clicks to search for PAM Health facilities near the zip code, "46077," PAM Health sends a SubscribedButtonClick event.

105. Importantly, the SubscribedButtonClick event illustrates that PAM Health enabled Advanced Matching Parameters, which "allow[s] Meta to connect collected event data to users, even if they do not have Facebook's browser cookies."[67] The SubscribedButtonClick event transmits the "udff[zp]" parameter, meaning that PAM Health includes a hashed version of the user's entered zip code in the SubscribedButtonClick event. Although the data is hashed, "[h]ashing does not prevent Meta from using this data to match people who visit websites to their Facebook profiles."[68]

[67] https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector#advanced-matching-parameters
[68] *Id.*

106. When the user loads a page about a hospital matching the user's search for facilities near zip code, "46077," PAM Health sends another PageView event, informing Facebook that the user is browsing a page about "pam-health-rehabilitation-hospital-greater-indiana."

PAM Health's Tracking and Disclosures of Users' Searches and Views of Services

107. As a final example of its disclosures, PAM Health also sends information to Facebook about users' search for services on PAM Health's website.

108. When a user navigates to view services offered by PAM Health, PAM Health sends a PageView event, alerting Facebook that the user is on the page, "https://pamhealth.com/health-services." Next, as the user opens a page about Parkinson's disease, PAM Health sends another PageView event, which informs Facebook the user is now on a page about "conditions/parkinsons."

109. PAM Health sends yet another PageView event to Facebook when the user then clicks to browse a page about PAM Health's rehabilitation hospital in Tulsa, which offers Parkinson's services. The PageView informs Facebook that the user opened the page about "rehabilitation-hospitals/pam-rehabilitation-hospital-tulsa" after viewing a page about "conditions/parkinsons."

110. Finally, when the user clicks to get directions to the Rehabilitation Hospital in Tulsa, PAM Health sends a FindLocation event, informing Facebook about that activity.

111. After receiving this information from Defendants, Facebook processes it, analyzes it, and assimilates it into its own massive datasets, before selling access to this data in the form of targeted advertisements. Employing "Audiences"—subsections of individuals identified as sharing common traits—Facebook promises the ability to "find the people most likely to respond

to your ad."[69] Advertisers can purchase the ability to target their ads based on a variety of criteria: "Core Audiences," individuals who share a location, age, gender, and/or language;[70] "Custom Audiences," individuals who have taken a certain action, such as visiting a website, using an app, or buying a product bought a product;[71] and/or "Lookalike Audiences," groups of individuals who "resemble" a Custom Audience, and who, as Facebook promises, "are likely to be interested in your business because they're similar to your best existing customers.[72]

112. Google and other companies process data in a similar manner and use it to build marketing and other data profiles allowing for targeted advertising.

113. Defendants could have chosen not to use the Meta Pixel, or it could have configured it to limit the information that it communicated to third parties, but it did not. Instead, it intentionally selected and took advantage of the features and functionality of the Pixel that resulted in the Disclosure of Plaintiff's and Class Members' Private Information.

114. Along those same lines, Defendants could have chosen not to use other tracking technologies such as MarketingCloudFX, Google Analytics with Google Tag Manager ("GTM"), Microsoft Clarity, and DoubleClick to track Plaintiff and Class Members private communications and transmit that information to unauthorized third parties. It did so anyway, intentionally taking advantage of these trackers despite the harm to Plaintiff's and Class Members' privacy.

115. Defendants used and disclosed Plaintiff's and Class Members' Private Information to Facebook, and to Google, MarketingCloudFX, Microsoft, and possibly other third parties, for the purpose of marketing their services and increasing its profits.

---

[69] Audience Ad Targeting, Meta, https://www.facebook.com/business/ads/ad-targeting (last visited Aug. 14, 2023).
[70] *Id.*
[71] *Id.*
[72] How to Create a Lookalike Audience on Meta Ads Manager, Meta Business Help Center, https://www.facebook.com/business/help/465262276878947 (last visited Aug. 14, 2023).

116. On information and belief, Defendants shared, traded, or sold Plaintiff's and Class Members' Private Information with Facebook, and potentially other third parties, in exchange for improved targeting and marketing services.

117. Plaintiff and the Class Members never consented, agreed, authorized, or otherwise permitted Defendants PAM Health to intercept their communications or to use or disclose their Private Information for marketing purposes. Plaintiff and the Class were never provided with any written notice that Defendants disclosed its patients' Protected Health Information to Facebook and others, such as Google, MarketingCloudFX, or Microsoft, nor were they provided any means of opting out of such disclosures. Defendants nonetheless knowingly disclosed Plaintiff's and the Class's Protected Health Information to unauthorized entities.

118. Plaintiff and Class Members relied on Defendants to keep their Private Information confidential and securely maintained, to use this information for legitimate healthcare purposes only, and to make only authorized disclosures of this information.

119. Furthermore, Defendants actively misrepresented that they would preserve the security and privacy of Plaintiff's and Class Members' Private Information. In actuality, Defendants shared data about Plaintiff's and Class Members' activities on the Online Platforms alongside identifying details about the Plaintiff and Class Members, such as their IP addresses.

120. By law, Plaintiff and the Class Members are entitled to privacy in their Protected Health Information and confidential communications. PAM Health deprived Plaintiff and Class Members of their privacy rights when they (1) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiff's and Class Members' confidential communications, Personally Identifiable Information, and Protected Health Information; (2) disclosed patients' Private Information to unauthorized, third-party eavesdroppers, including Facebook and possibly others;

and (3) undertook this pattern of conduct without notifying Plaintiff and Class Members and without obtaining their express written consent.

B. Plaintiff's Experience

121. Plaintiff's late wife, Jane Doe ("Mrs. Doe"), was a patient of Defendants beginning in 2019, receiving healthcare services from PAM Health and physicians in PAM Health's network for medical conditions including blood cancer, Atypical hemolytic uremic syndrome (aHUS), kidney issues, and inpatient hospital care including ventilation and coma care. Mrs. Doe received care from Defendants at PAM Health Specialty Hospital of Dayton, within Kettering Health Miamisburg.

122. Mrs. Doe passed away on March 29, 2021 in Dayton, Ohio, and Plaintiff is the Personal Representative of Mrs. Doe's Estate.

123. Plaintiff relied on PAM Health's Website and Online Platforms to communicate confidential patient information relating to Mrs. Doe, beginning in 2020, and last in December 2021, including to: search for treatments and medical information, topics related to the quality of care, and kidney, blood, respiratory, and wound doctors for Mrs. Doe;[73] to find locations;[74] to research treatments;[75] and to access the patient portal to message doctors and request information.[76]

124. Plaintiff accessed Defendants' Website and Online Platforms at Defendants' direction and encouragement on behalf of his wife, Mrs. Doe. Plaintiff reasonably expected that his and Mrs. Doe's online communications with PAM Health were confidential, solely between

[73] E.g., search for "amputation" avail. at https://pamhealth.com/search-results?search_paths%5B%5D=&query=amputation (last acc. Mar. 6, 2024).
[74] https://pamhealth.com/facilities (last acc. Mar. 6, 2024).
[75] https://pamhealth.com/health-services (last acc. Mar. 6, 2024).
[76] https://pamhealth.com/login (last acc. Mar. 6, 2024).

himself, Mrs. Doe's and PAM Health, and that, as such, those communications would not be transmitted to or intercepted by a third party.

125. Plaintiff provided his and Mrs. Doe's Private Information to Defendants and trusted that the information would be safeguarded according to PAM Health's Privacy Policies and the law.

126. Through its use of the Meta Pixel, Defendants disclosed to Facebook:

a. Plaintiff's and Mrs. Doe's identities via their IP addresses and/or "c_user" cookies;

b. The pages Plaintiff viewed for Mrs. Doe;

c. Plaintiff's seeking of medical treatment for Mrs. Doe;

d. Mrs. Doe's status as a patient;

e. Plaintiff's search terms on behalf of Mrs. Doe on the Online Platforms for treatments, medical information, topics related to the quality of care, and kidney, blood, respiratory, and wound doctors;

f. The locations and facilities and doctors which Plaintiff viewed for Mrs. Doe; and,

g. The medical treatment services Plaintiff viewed for Mrs. Doe.

127. By failing to receive the requisite consent, PAM Health breached confidentiality and unlawfully disclosed Plaintiff's and Mrs. Doe's Private Information.

128. Plaintiff first discovered that Defendants were using the Meta Pixel and other tracking technologies to gather and disclose his and Mrs. Doe's Private Information in December 2023.

129. As a result of PAM Health's Disclosure of Plaintiff's and Mrs. Doe's Private

Information via the Meta Pixel and other tracking technologies to third parties without authorization, he now receives targeted health-related advertisements reflecting private medical treatment information, including those related to skin conditions, arthritis, geriatric medical conditions, as well as for clinical trials, and physicians.

130. Plaintiff paid PAM Health for medical services for Mrs. Doe and the services he paid for included reasonable privacy and data security protections for his and her Private Information, but Plaintiff did not receive the privacy and security protections for which he paid, due to Defendants' Disclosure.

131. Because of Defendants' unauthorized Disclosure of his and Mrs. Doe's Private Information, Plaintiff has suffered injuries, including monetary damages; loss of privacy; unauthorized disclosure of this Private Information; unauthorized access to his and Mrs. Doe's Private Information by third parties; use of their Private Information for advertising purposes; embarrassment, humiliation, frustration, and emotional distress; decreased value of their Private Information; lost benefit of the bargain; and increased risk of future harm resulting from further unauthorized use and disclosure of their information.

C. Investigations and Reports Reveal the Meta Pixel's Impermissible Collection of PHI

132. In June 2020, after promising users that app developers would not have access to data if users were not active in the prior 90 days, Facebook revealed that it still enabled third-party developers to access this data.[77] This failure to protect users' data enabled thousands of developers to see data on inactive users' accounts if those users were Facebook friends with someone who was an active user.

133. On February 18, 2021, the New York State Department of Financial Services

[77] Kurt Wagner & Bloomberg, Facebook Admits Another Blunder with User Data, FORTUNE (July 1, 2020 at 6:30 p.m.) https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/.

released a report detailing the significant privacy concerns associated with Facebook's data collection practices, including the collection of health data. The report noted that while Facebook maintained a policy that instructed developers not to transmit sensitive medical information, Facebook received, stored, and analyzed this information anyway. The report concluded that "[t]he information provided by Facebook has made it clear that Facebook's internal controls on this issue have been very limited and were not effective . . . at preventing the receipt of sensitive data."[78]

134. The New York State Department of Financial Service's concern about Facebook's cavalier treatment of private medical data was not misplaced. In June 2022, the FTC finalized a different settlement involving Facebook's monetizing of sensitive medical data. In that case, the more than 100 million users of Flo, a period and ovulation tracking app, learned something startling: the company was sharing their data with Facebook.[79] When a user was having her period or informed the app of her intention to get pregnant, Flo would tell Facebook, which could then use the data for all kinds of activities including targeted advertising. In 2021, Flo settled with the Federal Trade Commission for lying to its users about secretly sharing their data with Facebook, as well as with a host of other internet advertisers, including Google, Fabric, AppsFlyer, and Flurry. The FTC reported that Flo "took no action to limit what these companies could do with users' information."[80]

135. More recently, Facebook employees admitted to lax protections for sensitive user data. Facebook engineers on the ad business product team conceded in a 2021 privacy review that

---

[78] New York State Department of Financial Services, REPORT ON INVESTIGATION OF FACEBOOK INC. DATA PRIVACY CONCERNS, (Feb. 18, 2021) https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf.
[79] Justin Sherman, Your Health Data Might Be for Sale, SLATE (June 22, 2022 at 5:50 a.m.) https://slate.com/technology/2022/06/health-data-brokers-privacy.html.
[80] *Id.*

"[w]e do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.'"[81]

136. Furthermore, in June 2022, an investigation by The Markup[82] revealed that the Meta Pixel was embedded on the websites of 33 of the top 100 hospitals in the nation.[83] On those hospital websites, the Meta Pixel collects and sends Facebook a "packet of data," including sensitive personal health information, whenever a user interacts with the website, for example, by clicking a button to schedule a doctor's appointment.[84] The data is connected to an IP address, which is "an identifier that's like a computer's mailing address and can generally be linked to a specific individual or household—creating an intimate receipt of the appointment request for Facebook."[85]

137. During its investigation, The Markup found that Facebook's purported "filtering" failed to discard even the most obvious forms of sexual health information. Worse, the article found that the data that the Meta Pixel was sending Facebook from hospital websites not only included details such as patients' medications, descriptions of their allergic reactions, details about their upcoming doctor's appointments, but also included patients' names, addresses, email addresses, and phone numbers.[86]

138. In addition to the 33 hospitals identified by The Markup that had installed the Meta

---

[81] Lorenzo Franceschi-Bicchierai, Facebook Doesn't Know What It Does with Your Data, or Where It Goes: Leaked Document, VICE (April 26, 2022) https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes.

[82] The Markup is a nonprofit newsroom that investigates how powerful institutions are using technology to change our society. *See* www.themarkup.org/about (last accessed Mar. 19, 2023).

[83] Todd Feathers, Simon Fondrie-Teitler, Angie Waller, & Surya Mattu, Facebook Is Receiving Sensitive Medical Information from Hospital Websites, THE MARKUP (June 16, 2022 6:00 a.m.) https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

[84] *Id.*

[85] *Id.*

[86] *Id.*

Pixel on their websites, The Markup identified seven health systems that had installed the Meta Pixel inside their password-protected patient portals.[87]

139. David Holtzman, health privacy consultant and former senior privacy adviser in the U.S. Department of Health and Human Services' Office for Civil Rights, stated he was "deeply troubled" by what the hospitals capturing and sharing patient data in this way.[88]

D. Defendants Violated HIPAA Standards

140. Under HIPAA, a healthcare provider may not disclose personally identifiable, non-public medical information (PHI) about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[89]

141. Guidance from the United States Department of Health and Human Services instructs healthcare providers that patient status alone is protected by HIPAA.

142. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[90]

143. In its guidance for Marketing, the Department further instructs:

The HIPAA Privacy Rule gives individuals important controls over whether and

---

[87] *Id.*
[88] *Id.*
[89] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).
[90] U.S. Department of Health and Human Services, Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, (Nov. 26, 2012) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

> how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list. (Emphasis added).[91]

144. In addition, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has issued a Bulletin to highlight the obligations of HIPAA-covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technology.[92]

145. According to the Bulletin, "HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information."[93]

146. Citing The Markup's June 2022 article, the Bulletin expressly notes:

> Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors. **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.** For example, disclosures of PHI to tracking technology vendors or marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.
>
> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to

---

[91] U.S. Department of Health and Human Services, Marketing, (Dec. 3, 2002) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf.

[92] *See* U.S. Department of Health and Human Services, Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/hipaa-online-tracking/index.html.

[93] *Id.*

> others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule. [94]

147. In other words, HHS has expressly stated that Defendants' conduct of implementing the Meta Pixel is a violation of HIPAA Rules.

E. Defendants Violated FTC Standards, and the FTC and HHS Take Action

148. The Federal Trade Commission ("FTC") has also recognized that implementation of the Meta Pixel and other tracking technologies pose "serious privacy and security risks" and "impermissibly disclos[e] consumers' sensitive personal health information to third parties."[95]

149. On July 20, 2023, the FTC and HHS sent a "joint letter to approximately 130 hospital systems and telehealth providers to alert them about the risks and concerns about the use of technologies, such as Meta/Facebook pixel and Google Analytics, that can track a user's online activities."[96]

150. Therein, the FTC reminded healthcare providers that "HIPAA regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to third parties or any other violations of the HIPAA Rules"[97] and that "[t]his is true even if you relied upon a third party to develop your website or mobile app and even if you

---

[94] *Id.* (emphasis in original) (internal citations omitted).
[95] Re: Use of Online Tracking Technologies, U.S. Dep't of Health & Human Services, (July 20, 2023) (available at https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf), **Exhibit A.**
[96] FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies, FEDERAL TRADE COMMISSION (July 20, 2023) https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking?utm_source=govdelivery.
[97] *Id.*

do not use the information obtained through use of a tracking technology for any marketing purposes."[98]

151. Entities that are not covered by HIPAA also face accountability for disclosing consumers' sensitive health information under the Health Breach Notification Rule. 16 C.F.R. § 318. This Rule requires that companies dealing with health records notify the FTC and consumers if there has been a breach of unsecured identifiable health information, or else face civil penalties for violations. *Id.* According to the FTC, "a 'breach' is not limited to cybersecurity intrusions or nefarious behavior. Incidents of unauthorized access, *including sharing of covered information without an individual's authorization*, triggers notification obligations under the Rule."[99]

152. Additionally, the FTC Act makes it unlawful to employ "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce[.]" 15 U.S.C. § 45(a). According to the FTC, "the disclosure of [sensitive health] information without a consumer's authorization can, in some circumstances, violate the FTC Act as well as constitute a breach of security under the FTC's Health Breach Notification Rule."[100]

153. As such, the FTC and HHS have expressly stated that conduct like Defendants' runs afoul of the FTC Act and/or the FTC's Health Breach Notification Rule.

---

[98] *Id.*

[99] Statement of the Commission: On Breaches by Health Apps and Other Connected Devices, U.S. Fed. Trade Commission, (Sept. 15, 2021) (available at https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf) (emphasis added).

[100] *See, e.g.*, U.S. v. Easy Healthcare Corp., Case No. 1:23-cv-3107 (N.D. Ill. 2023), https://www.ftc.gov/legallibrary/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v; In the Matter of BetterHelp, Inc., FTC Dkt. No. C-4796 (July 14, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter; U.S. v. GoodRx Holdings, Inc., Case No. 23-cv-460 (N.D. Cal. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc; In the Matter of Flo Health Inc., FTC Dkt. No. C-4747 (June 22, 2021), https://www.ftc.gov/legal-library/browse/casesproceedings/192-3133-flo-health-inc.

F. Defendants Violated Industry Standards

154. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient and hospital-patient relationship.

155. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications, which are applicable to PAM Health and its physicians.

156. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care . . . . Patient privacy encompasses a number of aspects, including . . . personal data (informational privacy).

157. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (a) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

158. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically . . . must . . . release patient information only in keeping ethics guidelines for confidentiality.

G. Plaintiff's and Class Members' Expectation of Privacy

159. At all times when Plaintiff and Class Members provided their Private Information to Defendants, they all had a reasonable expectation that the information would remain private and

that Defendants would not share the Private Information with third parties for a commercial marketing and sales purposes, unrelated to patient care.

H. IP Addresses are Personally Identifiable Information

160. Defendants also disclosed and otherwise assisted Facebook and potentially others with intercepting Plaintiff's and Class Members' IP addresses using the Meta Pixel and other tracking technologies.

161. An IP address is a number that identifies the address of a device connected to the Internet.

162. IP addresses are used to identify and route communications on the Internet.

163. IP addresses of individual Internet users are used by Internet service providers, Websites, and third-party tracking companies to facilitate and track Internet communications.

164. Facebook tracks every IP address ever associated with a Facebook user.

165. Facebook tracks IP addresses for use of targeting individual homes and their occupants with advertising.

166. Under HIPAA, an IP address is Personally Identifiable Information:

- HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).
- HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *See also*, 45 C.F.R. § 164.514(b)(2)(i)(O).

167. Consequently, by disclosing IP addresses, Defendants' business practices violated HIPAA and industry privacy standards.

I. Defendants Were Enriched and Benefitted from the Use of The Pixel and Unauthorized Disclosures

168. The sole purpose for Defendants' use of the Meta Pixel and other tracking technology was marketing and profits.

169. In exchange for disclosing the Private Information of its patients, Defendants is compensated by Facebook and likely others in the form of enhanced advertising services and more cost-efficient marketing on its platform.

170. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions. Upon information and belief, as part of its marketing campaign, Defendants re-targeted patients and potential patients.

171. By utilizing the Meta Pixel and other trackers, the cost of advertising and retargeting was reduced, thereby benefiting Defendants.

J. Plaintiff's and Class Members' Private Information Had Financial Value

172. The data concerning Plaintiff and Class Members, collected and shared by Defendants, has tremendous economic value. Data collected via the Meta Pixel, CAPI, and other online tracking tools allows Facebook to build its own massive, proprietary dataset, to which it then sells access in the form of targeted advertisements. Targeting works by allowing advertisers to direct their ads at particular "Audiences," subsets of individuals who, according to Facebook, are the "people most likely to respond to your ad."[101] Facebook's "Core Audiences" allow advertisers to target individuals based on demographics, such as age, location, gender, or language, whereas "Custom Audiences" allow advertisers to target individuals who have "already shown interest in your business," by visiting a business's website, using an app, or engaging in certain online content.[102] Facebook's "Lookalike Audiences" go further, targeting individuals who

[101] Audience Ad Targeting, Meta, https://www.facebook.com/business/ads/ad-targeting (last visited Aug. 14, 2023).
[102] *Id.*

resemble current customer profiles and whom, according to Facebook, "are likely to be interested in your business."[103]

173. Data harvesting is big business, and it drives Facebook's profit center, its advertising sales. In 2019, Facebook generated nearly $70 billion dollars in advertising revenue alone, constituting more than 98% of its total revenue for that year.[104]

174. This business model is not limited to Facebook. Data harvesting one of the fastest growing industries in the country, and consumer data is so valuable that it has been described as the "new oil." Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 were as high as $434 per user, for a total of more than $200 billion industry wide.

175. In particular, the value of health data is well-known due to the media's extensive reporting on the subject. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry." Therein, Time Magazine described the extensive market for health data and observed that the health data market is both lucrative and a significant risk to privacy.[105]

176. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[106]

---

[103] *See* How to Create a Lookalike Audience on Meta Ads Manager, Meta Business Center, https://www.facebook.com/business/help/465262276878947 (last visited Aug. 14, 2023).
[104] *See* Here's How Big Facebook's Ad Business Really Is, CNN, https://www.cnn.com/2020/06/30/tech/facebook-ad-business-boycott/index.html (last visited Aug. 14, 2023).
[105] *See* Adam Tanner, How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry, TIME, (Jan. 9, 2017 at 9:00 a.m.) https://time.com/4588104/medical-data-industry/.
[106] *See* Christina Farr, Hospital Execs Say They are Getting Flooded with Requests for Your Health Data, CNBC, (Dec. 18, 2019 at 8:27 a.m.) https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html.

TOLLING, CONCEALMENT, AND ESTOPPEL

177. The applicable statutes of limitation have been tolled as a result of PAM Health's knowing and active concealment and denial of the facts alleged herein.

178. PAM Health seamlessly incorporated Meta Pixel and other trackers into their Website and Online Platforms while providing users with no indication that their Website usage was being tracked and transmitted to third parties. PAM Health knew that their Website incorporated Meta Pixel and other trackers, yet it failed to disclose to Plaintiff and Class Members that their sensitive medical information would be intercepted, collected, used by, and disclosed to Facebook, Google, MarketingCloudFX, Microsoft Clarity, and likely other third parties.

179. Plaintiff and Class Members could not with due diligence have discovered the full scope of PAM Health's conduct, because there were no disclosures or other indication that they were interacting with websites employing Meta Pixel or any other tracking technology.

180. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrine of continuing tort. PAM Health's illegal interception and disclosure of Plaintiff's and Mrs. Doe's Private Information has continued unabated, at least up until November 2023 if not later. What is more, PAM Health was under a duty to disclose the nature and significance of their data collection practices but did not do so. PAM Health is therefore estopped from relying on any statute of limitations defenses.

CLASS ALLEGATIONS

181. Plaintiff brings this nationwide class action individually, as Personal Representative of the Estate of Jane Doe (hereinafter, collectively, "Plaintiff") and on behalf of all other similarly situated persons.

182. The nationwide Class that Plaintiff seeks to represent is defined as follows:

All persons whose Private Information was disclosed by Defendants to third parties through the Meta Pixel and related technology without authorization.

183. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers, and directors, and any entity in which Defendants has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state, or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels, and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

184. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

185. Numerosity: Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds or thousands of individuals whose Private Information may have been improperly used or disclosed by Defendants, and the Class is identifiable within Defendants' records.

186. Commonality: Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. whether and to what extent Defendants had a duty to protect Plaintiff's and Class Members' Private Information;

b. whether Defendants had duties not to disclose the Plaintiff's and Class Members' Private Information to unauthorized third parties;

c. whether Defendants had duties not to use Plaintiff's and Class Members'

Private Information for non-healthcare purposes;

d. whether Defendants had duties not to use Plaintiff's and Class Members' Private Information for unauthorized purposes;

e. whether Defendants failed to adequately safeguard Plaintiff's and Class Members' Private Information;

f. whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

h. whether Defendants failed to properly implement and configure the tracking software on its Online Platforms to prevent the disclosure of confidential communications and Private Information;

i. whether Defendants breached their duties of care to Plaintiff and the Class Members and were negligent;

j. whether Defendants committed invasion of privacy—intrusion upon seclusion;

k. whether Defendants committed invasion of privacy—public disclosure of private facts;

l. whether Defendants breached their contract with Plaintiff and the Class Members; or in the alternate, whether Defendants were unjustly enriched;

m. whether Defendants owed fiduciary duties to the Plaintiff and the Class Members;

n. whether Defendants breached fiduciary duties;

o. whether Defendants engaged in unfair, unlawful, or deceptive practices by misrepresenting that it would safeguard Plaintiff's and Class Members' Private Information;

p. whether Defendants violated the Pennsylvania Unfair Trade Practices And Consumer Protection Law, 73 Pa. Stat. § 20101, *et. seq.* ("UTPCPL");

q. whether Defendants violated the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. C.S. § 5701, *et. seq.* ("WESCA"); and,

r. whether Plaintiff and the Class Members are entitled to monetary damages, including compensatory and statutory damages, and the sums thereof.

187. Typicality: Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendants' use and incorporation of Meta Pixel and other tracking technology.

188. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly, and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

189. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the

Class Members and the infringement of the rights and the damages Plaintiff has suffered is typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

190. Superiority and Manageability: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

191. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged. If the class action device were not used, Defendants would necessarily gain an unconscionable advantage because they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources. Moreover, the costs of individual suits could unreasonably consume the amounts that would be recovered, whereas proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged. Finally, individual actions would create a risk of inconsistent results and would be unnecessary and

duplicative of this litigation.

192. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

193. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

194. Unless a Class-wide injunction is issued, Defendants may continue in its unlawful use and disclosure and failure to properly secure the Private Information of Class Members, Defendants may continue to refuse to provide proper notification to and obtain proper consent from Class Member, and Defendants may continue to act unlawfully as set forth in this Complaint.

195. Further, Defendants has acted or refused to act on grounds generally applicable to the Class, and, accordingly, final injunctive or corresponding declaratory relief regarding the whole of the Class is appropriate.

196. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

a. whether Defendants owed a legal duty to Plaintiff and the Class Members to not disclose their nonpublic medical information, Private Information, to third parties without Plaintiff's or the Class Members' informed consent or other legal privilege;

b. whether Defendants disclosed Plaintiff's and the Class Members' nonpublic

medical information, Private Information, to third parties without their informed consent or applicable legal privilege;

c. whether Defendants owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

d. whether Defendants breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

e. whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to the disclosure of patient information;

f. whether Defendants failed to implement and maintain reasonable security procedures and practices;

g. whether Defendants adequately and accurately informed Plaintiff and Class Members that their Private Information had been used and disclosed to third parties;

h. whether Defendants were negligent;

i. whether an implied contract existed between Defendants on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

j. whether Defendants breached the implied contract;

k. whether Defendants were unjustly enriched;

l. whether Defendants committed an invasion of privacy—intrusion upon

seclusion;

m. whether Defendants committed an invasion of privacy—public disclosure of private facts;

n. whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' Private Information;

o. whether Defendants violated the Pennsylvania Unfair Trade Practices And Consumer Protection Law, 73 Pa. Stat. § 20101, *et. seq.* ("UTPCPL");

p. whether Defendants violated the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. C.S. § 5701, *et. seq.* ("WESCA"); and,

q. whether Plaintiff and the Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

197. Plaintiff realleges and incorporates the above allegations as if fully set forth herein.

198. Defendants owed to Plaintiff and Class Members a duty to exercise reasonable care in handling and using Plaintiff's and Class Members' Private Information in its care and custody, including implementing industry-standard privacy procedures sufficient to reasonably protect the information from the disclosure and unauthorized transmittal and use of Private Information that occurred.

199. Defendants acted with wanton and reckless disregard for the privacy and confidentiality of Plaintiff's and Class Members' Private Information by disclosing and providing access to this information to third parties for the financial benefit of the third parties and

Defendants.

200. Defendants owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' disclosure of their Private Information to benefit third parties and Defendants. Defendants actively sought and obtained Plaintiff's and Class Members' Private Information.

201. Private Information is highly valuable, and Defendants knew, or should have known, the harm that would be inflicted on Plaintiff and Class Members by disclosing their Private Information to third parties. This disclosure was of benefit to third parties and Defendants by way of data harvesting, advertising, and increased sales.

202. Defendants breached their duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and Private Information of Plaintiff and Class Members. This failure actually and proximately caused Plaintiff's and Class Members' injuries.

203. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, inappropriate advertisements and use of their Private Information for advertising purposes, and increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

204. Defendants' breach of their common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff's and Class Members' actual, tangible, injury-in-fact and damages, including, without limitation, the unauthorized access of their Private Information by third parties, improper disclosure of their Private Information, lost benefit

of their bargain, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of use of their information that resulted from and were caused by Defendants' negligence. These injuries are ongoing, imminent, immediate, and continuing.

205. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class are entitled to recover damages including actual and compensatory damages, and punitive damages, as permitted by law.

COUNT II
INVASION OF PRIVACY--INTRUSION UPON SECLUSION
(On Behalf of Plaintiff and the Class)

206. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

207. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendants via their Website and the communications platforms and services therein.

208. Plaintiff and Class Members communicated sensitive Private Information, PHI and PII, that they intended for only Defendants to receive and that they understood Defendants would keep private.

209. Defendants' disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiff and Class Members is an intentional intrusion on Plaintiff's and Class Members' solitude or seclusion and their private affairs and concerns.

210. Plaintiff and Class Members had a reasonable expectation of privacy given Defendants' representations, Notice of Privacy Practices, Terms of Use, and HIPAA. Moreover, Plaintiff and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential. Defendants' disclosure of PHI

coupled with PII is highly offensive to the reasonable person.

211. As a result of Defendants' actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to invasion of their privacy rights, the unauthorized access of their Private Information by third parties, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of use of their information that resulted from and were caused by Defendants' conduct. These injuries are ongoing, imminent, immediate, and continuing.

212. Plaintiff and Class Members have been damaged as a direct and proximate result of Defendants' invasion of their privacy and are entitled to just compensation, including monetary damages.

213. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as a result of its intrusions upon Plaintiff's and Class Members' privacy.

214. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendants' actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendants from engaging in such conduct in the future.

215. Plaintiff also seek such other relief as the Court may deem just and proper.

COUNT III
INVASION OF PRIVACY—PUBLIC DISCLOSURE OF PRIVATE FACTS
(On Behalf of Plaintiff and the Class)

216. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

217. In the Disclosure, Defendants publicized private details and facts not generally known to the public, not publicly available, and not of legitimate public concern about Plaintiff

and the Class by disclosing and exposing Plaintiff's and the Class's Private Information, including sensitive medical information, to enough people that it is reasonably likely those facts will become known to the public at large.

218. The disclosure of patients' Private Information, including PHI such as medical conditions and treatments viewed, and identifying information, is particularly harmful and would be offensive to a reasonable person of ordinary sensibilities.

219. Defendants have a special relationship with Plaintiff and Class Members and Defendant's disclosure of Private Information as described herein is certain to embarrass them and offend their dignity. Defendants should appreciate that the Disclosure would result in dissemination of Private Information to unauthorized parties.

220. The tort of public disclosure of private facts is recognized in Pennsylvania. *See Harris by Harris v. Easton Pub. Co.*, 335 Pa. Super. 141, 154, 483 A.2d 1377 (1984). Plaintiff's and the Class's Private Information was publicly disclosed by Defendant in the Disclosure intentionally and/or with reckless disregard for the reasonable offensiveness of the disclosure.

221. Such Disclosure is highly offensive and would be to any person of ordinary sensibilities. Defendant knew or should have known that Plaintiff's and the members of the Class's PII is not a matter of legitimate public concern.

222. As a direct and proximate result of Defendants' conduct, Plaintiff and members of the Class have suffered injury-in-fact and damages, including, without limitation, the unauthorized access of their Private Information by third parties, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of use of their information that resulted from and were caused by Defendants' conduct. These injuries are ongoing, imminent, immediate, and

continuing.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Class)

223. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

224. As a condition of receiving medical care from Defendants, Plaintiff and the Class provided their Private Information and paid compensation for the treatment received. In so doing, Plaintiff and Class Members entered into contracts with Defendants by which Defendants agreed to safeguard and protect such information, in their Privacy Policies and elsewhere, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

225. Implicit in the agreement between PAM Health and their patients, Plaintiff and the proposed Class Members, was the obligation that both parties would maintain the Private Information confidentially and securely.

226. PAM Health had an implied duty of good faith to ensure that the Private Information of Plaintiff and Class Members in its possession was only used only as authorized, such as to provide medical treatment, billing, and other medical benefits from PAM Health.

227. PAM Health had an implied duty to protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses.

228. Additionally, PAM Health implicitly promised to retain this Private Information only under conditions that kept such information secure and confidential.

229. Plaintiff and Class Members fully performed their obligations under the implied contract with PAM Health. Defendants did not. Plaintiff and Class Members would not have provided their confidential Private Information to PAM Health in the absence of their implied

contracts with PAM Health and would have instead retained the opportunity to control their Private Information for uses other than receiving medical treatment from PAM Health.

230. PAM Health breached the implied contracts with Plaintiff and Class Members by disclosing Plaintiff's and Class Members' Private Information to an unauthorized third party.

231. PAM Health's acts and omissions have materially affected the intended purpose of the implied contracts requiring Plaintiff and Class Members to provide their Private Information in exchange for medical treatment and benefits.

232. As a direct and proximate result of Defendants' above-described breach of contract, Plaintiff and the Class have suffered (and will continue to suffer) the compromise and disclosure of their Private Information and identities, as well as the unauthorized access of their Private Information by third parties, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of use of their information that resulted from and were caused by Defendants' breach of contract. These injuries are ongoing, imminent, immediate, and continuing.

233. As a direct and proximate result of Defendants' above-described breach of contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

234. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

235. This claim is pleaded solely in the alternative to Plaintiff's Breach of Implied Contract claim.

236. Plaintiff and Class Members conferred a monetary benefit upon PAM Health in the form of valuable sensitive medical information that Defendants collected from Plaintiff and Class

Members under the guise of keeping this information private. Defendants collected, used, and disclosed this information for its own gain, including for advertisement purposes, sale, or trade for valuable services from third parties. Additionally, Plaintiff and the Class Members conferred a benefit on Defendants in the form of monetary compensation paid in exchange for treatment, a part of which included payments for reasonable data security.

237. Plaintiff and Class Members would not have used PAM Health's services or would have paid less for those services, if they had known that Defendants would collect, use, and disclose their Private Information to third parties.

238. PAM Health appreciated or had knowledge of the benefits conferred upon them by Plaintiff and Class Members.

239. As a result of PAM Health's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

240. The benefits that Defendants derived from Plaintiff and Class Members rightly belong to Plaintiff and Class Members themselves. It would be inequitable under unjust enrichment principles for Defendants to be permitted to retain any of the profit or other benefits they derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

241. PAM Health should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds it received as a result of its conduct and the unauthorized Disclosure alleged herein.

COUNT VI
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

242. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

243. A relationship existed between Plaintiff and the Class, on the one hand, and Defendants, on the other, in which Plaintiff and the Class put their trust in Defendants to protect the Private Information of Plaintiff and the Class, and Defendants accepted that trust.

244. Defendants breached the fiduciary duty that they owed to Plaintiff and the Class Members by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect, and intentionally disclosing, their Private Information.

245. Defendants' breach of fiduciary duty was a legal cause of injury-in-fact and damage to Plaintiff and the Class, including but not limited to, the unauthorized access of their Private Information by third parties, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of use of their information that resulted from and were caused by Defendants' breach of fiduciary duty. These injuries are ongoing, imminent, immediate, and continuing.

246. But-for Defendants' breach of fiduciary duty, the injury-in-fact and damage to Plaintiff and the Class would not have occurred.

247. Defendants' breach of fiduciary duty contributed substantially to producing the damage to the Plaintiff and the Class.

248. As a direct and proximate result of Defendants' breach of fiduciary duty, Plaintiff and Class Members are entitled to and do demand actual, consequential, and nominal damages, injunctive relief, and all other relief allowed by law.

COUNT VII
VIOLATION OF THE PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, 73 PA. STAT. § 20101 *ET. SEQ.* ("UTPCPL")
(On Behalf of Plaintiff and the Class)

249. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

250. Plaintiff, Class Members, and Defendants are all "persons" within the meaning of the Pennsylvania Unfair Trade Practices and Consumer Protection Law ("UTPCPL"), 73 Pa. Stat. § 201-2(2).

251. The UTPCPL prohibits "unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce."

252. Under the UTPCPL, "[u]nfair or deceptive acts or practices" include: "[r]epresenting that . . . services have sponsorship, approval, characteristics, . . . [or] benefits . . . that they do not have," 73 Pa. § 201-2(4)(v); "[r]epresenting that… services are of a particular standard . . . [or] quality . . . if they are of another," *id.* § 201-2(4)(vii); "[a]dvertising… services with intent not to sell them as advertised," *id.* § 201-2(4)(ix); and "[e]ngaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding," *id.* § 201-2(4)(xxi).

253. Defendants' acts, practices, and omissions alleged in this Complaint constitute unlawful, unfair, and deceptive acts and practices under the UTPCPL.

254. Defendants knew or should have known about the unauthorized Disclosure of Plaintiff's and the Class's Private Information via the Meta Pixel, yet Defendants concealed that information from Plaintiff and the Class.

255. Defendants engaged in unlawful, unfair, and deceptive acts and practices prohibited by the UTPCPL by, among other things: misrepresenting or omitting material facts to Plaintiff and the Class regarding the adequacy of Defendants' protection of their Private Information, in

violation of 73 Pa. Stat. §§ 201-(4)(v), (vii), (ix), and (xxi);

256. Defendants' acts and omissions and its misrepresentations were intentional, knowing, and undertaken to mislead the public, including Plaintiff and the members of the Class.

257. Defendants' unlawful, unfair, and deceptive acts and practices were unethical, oppressive, and unscrupulous. These acts and practices caused substantial injury to Plaintiff and members of the Class that they could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

258. Defendants possessed exclusive knowledge about the Disclosure of Plaintiff's and the Class Member's Private Information to unauthorized parties via the Meta Pixel to their detriment.

259. Defendants had a duty to disclose the foregoing to Plaintiff and Class Members and failed to do so.

260. Plaintiff and members of the Class reasonably relied on Defendants to protect and safeguard their Private Information and to promptly and adequately inform them of the unauthorized Disclosure.

261. Defendants owed Plaintiff and the Class duties to maintain the privacy and security of Plaintiff's and the Class's Private Information; take proper action to prevent the Disclosure; take proper action following the Disclosure to protect further unauthorized disclosure, release, and theft of Private Information, and promptly inform Plaintiff and members of the Class about the Disclosure.

262. Plaintiff and members of the Class suffered ascertainable losses of money or property as a result of Defendants' use and employment of methods, acts, or practices declared to be unlawful by 73 Pa. §§ 201-2(2) and 201-(3).

263. Plaintiff and the Class seek an order enjoining Defendants' unlawful acts and practices and awarding any other just and proper relief available under the UTPCPL including actual or statutory damages, treble damages, and attorneys' fees and costs.

COUNT VIII
VIOLATION OF THE PENNSYLVANIA WIRETAPPING AND ELECTRONIC SURVEILLANCE CONTROL ACT 18 PA. C.S. § 5701, *ET SEQ.* ("WESCA")
(On Behalf of Plaintiff and the Class)

264. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

265. The Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. C.S.A. §§ 5701, 5703(1) ("WESCA") prohibits any person from willfully intercepting, endeavoring to intercept, or procuring of any other person to intercept or endeavor to intercept, any wire, electronic, or oral communication.

266. WESCA defines "Person" as any employee, or agent of the United States or any state or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation. 18 Pa. C.S.A. § 5702.

267. Defendants each constitute a "person" under WESCA, 18 Pa. C.S.A. § 5702.

268. WESCA, 18 Pa. C.S.A. § 5702 defines "intercept," as "[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." 18 Pa. C.S.A. § 5702.

269. WESCA, 18 Pa. C.S.A. § 5703(2)-(3) also prohibits the disclosure of, or use of, the contents of any wire, electronic, or oral communication, or any evidence derived therefrom, with knowledge that the information was obtained through the interception of a wire, electronic, or oral communication.

270. WESCA, 18 Pa. C.S.A. § 5741(a) further prohibits the knowing access without authorization of a facility through which an electronic communication is provided or exceeds an

authorization to access that facility and obtains, or alters access to a wire or electronic communication while that communication is in electronic storage.

271. WESCA, 18 Pa. C.S.A. § 5741, is also violated where, for the purpose of commercial advantage or private commercial gain, a person knowingly accesses without authorization a facility through which an electronic communication service is provided, or exceed access to that facility, and obtains access to a wire or electronic communication while that communication is in electronic storage.

272. As set forth herein, Defendants knowingly, willfully, and intentionally intercepted and disclosed Plaintiff's and Class Members' electronic communications, without the consent of the Plaintiff and Class Members, using Facebook's and other third parties' tracking devices.

273. Defendants knowingly, willfully, and intentionally intercepted Plaintiff's and Class Members' electronic communications for the purpose of disclosing those communications to third parties including Facebook and others without the knowledge, consent, or written authorization of Plaintiff or Class Members.

274. The devices used in this case, include, but are not limited to:

a. those to which Plaintiff's and Class Members' communications were disclosed;

b. Plaintiff's and Class Members' personal computing devices;

c. Plaintiff's and Class Members' web browsers;

d. Plaintiff's and Class Members' browser-managed files;

e. the Meta Pixel;

f. internet cookies;

g. other pixels, trackers, and/or tracking technology installed on Defendants'

Website and/or server;

h. Defendants' computer servers;

i. third-party source code utilized by Defendants; and

j. computer servers of third parties (including Facebook).

275. Defendants aided in the interception of communications between Plaintiff and Class Members and Defendants that were redirected to and recorded by third parties without the Plaintiff's or Class Members' consent.

276. WESCA confers a private civil cause of action to any person whose wire, electronic or oral communication is intercepted, disclosed or used in violation thereof against "any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication." 18 Pa. C.S. § 5725(a).

277. As a result of Defendants' violations of WESCA, pursuant to 18 Pa. C.S.A. § 5725(a), Plaintiff and the Class Members are entitled to recover actual damages that are not less than liquidated damages computed at a rate of $100.00 a day for each day of violation or $1,000.00, whichever is higher; punitive damages; and reasonable attorneys' fees and other litigation costs reasonably incurred.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, JOHN DOE, Individually, as Personal Representative of the Estate of JANE DOE, and on behalf of all others similarly situated, prays for judgment as follows:

A. For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and Plaintiff's counsel as Class Counsel;

B. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law, including pursuant to the

Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 Pa. Stat. § 20101, *et seq.* ("UTPCPL"), and the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. C.S.A. §§ 5701, *et seq.* ("WESCA");

C. For an award of punitive damages, as allowable by law;

D. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

E. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Sensitive Information compromised during the Disclosure;

F. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

G. Ordering Defendants to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

H. For an award of attorneys' fees under the UTPCPL, WESCA, the common fund doctrine, and any other applicable law;

I. Costs and any other expense, including expert witness fees incurred by Plaintiff in connection with this action;

J. Pre- and post-judgment interest on any amounts awarded;

K. Trial by jury on all issues so triable; and,

L. Such other and further relief as this court may deem just and proper.

Dated: March 8, 2024

Respectfully submitted,

SALTZ MONGELUZZI & BENDESKY P.C.

By: */s/ Patrick Howard*

Patrick Howard (PA Atty ID #88572)
1650 Market Street, 52nd Floor
Pennsylvania, Pennsylvania 19103
(215) 496-8282
phoward@smbb.com

Lynn A. Toops (*Pro Hac Vice* forthcoming)
Mary Kate Dugan (*Pro Hac Vice* forthcoming)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com

J. Gerard Stranch, IV (*Pro Hac Vice* forthcoming)
Andrew E. Mize (*Pro Hac Vice* forthcoming)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com

Samuel J. Strauss (*Pro Hac Vice* forthcoming)
Raina C. Borelli (*Pro Hac Vice* forthcoming)
TURKE & STRAUSS, LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703
(608) 237-1775
(608) 509-4423 (facsimile)
sam@turkestrauss.com
raina@turkestrauss.com

Counsel for Plaintiff and the Proposed Class

EXHIBIT A

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

July 20, 2023

[Company]
[Address]
[City, State, Zip Code]
Attn: [Name of Recipient]

Re: Use of Online Tracking Technologies

Dear [Name of Recipient],

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) are writing to draw your attention to serious privacy and security risks related to the use of online tracking technologies that may be present on your website or mobile application (app) and impermissibly disclosing consumers' sensitive personal health information to third parties.

Recent research,[1] news reports,[2] FTC enforcement actions,[3] and an OCR bulletin[4] have highlighted risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These tracking technologies

---

[1] *See, e.g.*, Mingjia Huo, Maxwell Bland, and Kirill Levchenko, *All Eyes on Me: Inside Third Party Trackers' Exfiltration of PHI from Healthcare Providers' Online Systems*, Proceedings of the 21st Workshop on Privacy in the Electronic Society (Nov. 7, 2022), https://dl.acm.org/doi/10.1145/3559613.3563190.

[2] *See, e.g.*, Todd Feathers, Katie Palmer, and Simon Fondrie-Teitler, *Out of Control: Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, THE MARKUP (Dec. 13, 2022), https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies.

[3] *U.S. v. Easy Healthcare Corp.*, Case No. 1:23-cv-3107 (N.D. Ill. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v; *In the Matter of BetterHelp, Inc.*, FTC Dkt. No. C-4796 (July 14, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter; *U.S. v. GoodRx Holdings, Inc.*, Case No. 23-cv-460 (N.D. Cal. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc; *In the Matter of Flo Health Inc.*, FTC Dkt. No. C-4747 (June 22, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc.

[4] U.S. Dept. of Health and Human Svcs. Office for Civil Rights, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

gather identifiable information about users as they interact with a website or mobile app, often in ways which are not avoidable by and largely unknown to users.

Impermissible disclosures of an individual's personal health information to third parties may result in a wide range of harms to an individual or others. Such disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more. In addition, impermissible disclosures of personal health information may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

If you are a covered entity or business associate ("regulated entities") under HIPAA, you must comply with the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules), with regard to protected health information (PHI) that is transmitted or maintained in electronic or any other form or medium.

The HIPAA Rules apply when the information that a regulated entity collects through tracking technologies or discloses to third parties (*e.g.*, tracking technology vendors) includes PHI. HIPAA regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to third parties or any other violations of the HIPAA Rules. OCR's December 2022 bulletin about the use of online tracking technologies by HIPAA regulated entities provides a general overview of how the HIPAA Rules apply.[5] This bulletin discusses what tracking technologies are and reminds regulated entities of their obligations to comply with the HIPAA Rules when using tracking technologies.

FTC Act and FTC Health Breach Notification Rule

Even if you are not covered by HIPAA, you still have an obligation to protect against impermissible disclosures of personal health information under the FTC Act and the FTC Health Breach Notification Rule. This is true even if you relied upon a third party to develop your website or mobile app and even if you do not use the information obtained through use of a tracking technology for any marketing purposes. As recent FTC enforcement actions demonstrate, it is essential to monitor data flows of health information to third parties via technologies you have integrated into your website or app.[6] The disclosure of such information without a consumer's authorization can, in some circumstances, violate the FTC Act as well as constitute a breach of security under the FTC's Health Breach Notification Rule.[7] Within the last

---

[5] *Id.*

[6] *See supra* note 3.

[7] *See* Federal Trade Comm'n, *Statement of the Commission on Breaches by Health Apps and Other Connected Devices* (Sept. 15, 2021), https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf.

few months, the FTC has issued a series of guidance pieces addressed to entities collecting, using, or disclosing sensitive health information.[8]

OCR and the FTC remain committed to ensuring that consumers' health privacy remains protected with respect to this critical issue. Both agencies are closely watching developments in this area. To the extent you are using the tracking technologies described in this letter on your website or app, we strongly encourage you to review the laws cited in this letter and take actions to protect the privacy and security of individuals' health information.[9]

Sincerely,

/s/

Melanie Fontes Rainer
Director
Office for Civil Rights
U.S. Department of Health and Human Services

/s/

Samuel Levine
Director
Bureau of Consumer Protection
Federal Trade Commission

---

[8] *See, e.g.*, FTC Office of Technology, *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking* (Mar. 16, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking; Lesley Fair, *First FTC Health Breach Notification Rule case addresses GoodRx's not-so-good privacy practices* (Feb. 1, 2023), https://www.ftc.gov/business-guidance/blog/2023/02/first-ftc-health-breach-notification-rule-case-addresses-goodrxs-not-so-good-privacy-practices; Federal Trade Comm'n and the U.S. Department of Health & Human Services' Office of the National Coordinator for Health Information Technology (ONC), Office for Civil Rights (OCR), and Food and Drug Administration (FDA), *Mobile Health App Interactive Tool* (Dec. 2022), https://www.ftc.gov/business-guidance/resources/mobile-health-apps-interactive-tool; Kristin Cohen, *Location, health, and other sensitive information: FTC Committed to fully enforcing the law against illegal use and sharing of highly sensitive data* (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal.

[9] In addition to the HIPAA Rules, the FTC Act, and the FTC Health Breach Notification Rule, you may also be subject to other state or federal statutes that prohibit the disclosure of personal health information.

EXHIBIT B

Effective September 13, 2013

POST ACUTE MEDICAL LLC
NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY

The terms of this Notice of Privacy Practices apply to Post Acute Medical, LLC and each of its subsidiaries, affiliates, and entities managed or controlled by Post Acute Medical, including the corporate office and its employees. All of the entities will share personal health information of patients as necessary to carry out treatment, payment, and health care operations as permitted by law. Use or disclosure pursuant to this Notice may include electronic transmittal or disclosure of your personal health information.

Should we make a change, you may obtain a revised copy from the location providing treatment.

WE HAVE A LEGAL DUTY TO SAFEGUARD YOUR PROTECTED HEALTH INFORMATION (PHI)

We are legally required to protect the privacy of your health information. We call this information protected health information, or PHI for short and it includes information that can be used to identify you that we have created or received about your past, present, or future health or condition, the provision of health care to you, or the payment of this health care. We must provide you with this notice about our privacy practices that explains how, when, and why we use and disclose your PHI. With some exceptions, we may not use or disclose any more of your PHI than is necessary to accomplish the purpose of the use or disclosure. We are legally required to follow the privacy practices that are described in this notice as long as it remains in effect.

However, we reserve the right to change the terms of this notice and our privacy policies at any time. Any changes will apply to the PHI we already have. Should we make a change, you may obtain a revised copy from the Privacy Officer or the location providing treatment. The notice will contain on the first page, in the top right-hand corner, the effective date.

USES AND DISCLOSURES OF YOUR PROTECTED HEALTH INFORMATION

- Authorization. We will not use or disclose your PHI for any purpose other than treatment, payment and healthcare operations, unless you have a signed form authorizing the use or disclosure, with exception to the situations outlined below. You have the right to revoke that authorization in writing and we will no longer use or disclose medical information about you for the reasons covered by your written authorization. You understand that we are unable to take back any disclosures we have already made with your permission, and that we are required to retain our records of the care that we provided to you.
- Uses and Disclosures for Treatment. We may use and disclose your PHI as necessary for your treatment. For example, physicians, nurses and other health care professionals involved in your care will use information in your medical record and medical information that you provide to plan your course of treatment. This may include procedures, medications, tests, etc.
- Uses and Disclosures for Payment. We may use and disclose your PHI in order to bill and collect payment for the treatment and services provided to you. For example, we may provide portions of your PHI to our billing department and your health plan to get paid for the health care services we provided to you. We may also provide your PHI to our business associates, such as billing companies, claims processing companies, and others that process our health care claims and/or assist in payment collection activities.
- Uses and Disclosures for Health Care Operations. We may use and disclose your PHI as necessary, and as permitted by law, for our health care operations. For example, we may use your PHI in order to evaluate the quality of health care services that you received or to evaluate the performance of the health care professionals who provided health care services to you. We may also provide your PHI to our accountants, attorneys, consultants, and others in order to make sure we are complying with the laws that affect us.

CERTAIN USES AND DISCLOSURES DO NOT REQUIRE YOUR AUTHORIZATION

We may use and disclose your PHI without your authorization for the following reasons:

- Public health activities
- Health oversight activities
- Purposes of organ donation
- Research
- To avoid harm
- Specific government functions
- When required by federal, state or local law, judicial or administrative proceedings or law enforcement.
- Workers' Compensation
- Fundraising
- Business Associates
- Data breach notification
- Future communications
- Inmates or individuals in custody
- Appointment reminders and health related benefits or services.

USES AND DISCLOSURES THAT REQUIRE YOU HAVE THE OPPORTUNITY TO OBJECT

- Patient Directories. We may include your name, location in this facility, general condition, and religious affiliation in our patient directory for use by clergy and visitors who ask for you by name unless you object in whole or in part. The opportunity to consent may be obtained retroactively in emergencies.
- Family and Friends Involved in Your Care. We may provide your PHI to a family member, friend, or other person that you indicate is involved in your care or the payment for your health care, unless you object in whole or in part. If you are unavailable, incapacitated, or facing and emergency medical situation, we may disclose such information as necessary if we determine that it is in your best interest based on our professional judgment.
- Disaster Relief. We may disclose your PHI to disaster relief organizations that seek your PHI to coordinate your care, or notify family and friends of your location or condition in a disaster.

RIGHTS YOU HAVE REGARDING YOUR PHI

- Access to Your Protected Health Information. In most cases, you have the right to look at or get copies of your PHI that we have. Usually, this includes medical and billing records, but does not include psychotherapy notes. To inspect and/or receive copies of medical information that may be used to make decisions about you, you must submit your request in writing to the Privacy Officer or Medical Records Department. If your PHI is created and maintained in an electronic format, you have the right to request that an electronic copy of your record be given to you or transmitted to another individual or entity. We will make every effort to provide access to your PHI in the form or format you request, if it is readily producible in such form or format. If you request copies of your PHI, we may charge a fee for the costs of copying, transmitting, mailing or other supplies associated with your request. Instead of providing the PHI you requested, we may provide you with a summary or explanation of the PHI as long as you agree to that and to the cost in advance.
- Right to Request Limits on Uses and Disclosures of Your PHI. You have the right to ask that we limit how we use and disclose your PHI. We will consider your request but are not legally required to accept it. If we accept your request, we will put any limits in writing and abide by them except in emergency situations. You may not limit the uses and disclosures that we are legally required or allowed to make. To request restrictions, you must make your request in writing to the Privacy Officer. In your request, you must tell us (1) what information you want to limit; (2) whether you want to limit our use, disclosure or both; and (3) to whom you want the limits to apply, for example, disclosures to your spouse.
- Right to Request How We Send PHI to You. You have the right to ask that we send information to you to an alternate address (for example, sending information to your work address rather than your home address) or by alternate means (for example, e-mail instead of regular mail). We will honor your request so long as we can easily provide it in the format you requested.
- Right to an Accounting of the Disclosures We Have Made. You have the right to get a list of certain instances in which we have disclosed your PHI. Requests must be made in writing and must state a time period, which may not be longer than six years. We will respond within 60 days of receiving your request. The first accounting in any 12-month period is free. However, we may charge a fee for each subsequent accounting you make in the same year.
- Right to Amend or Update Your PHI. If you believe that there is a mistake in your PHI or that a piece of important information is missing, you have the right to request that we correct the existing information or add the missing information. You must provide the request and your reason for the request in writing to the Privacy Officer or Medical Records Department. We are not obligated to make all requested amendments but will give each request careful consideration. If we approve your request, we will make the change to your PHI and may notify others who work with us and have copies of the uncorrected record if we believe that such notification is necessary.
- The Right to Get Notice of a Breach. In the event of any breach of unsecured PHI, we will comply with the HIPAA/HITECH breach notification requirements, which will include notification to you.
- Out-of-Pocket Payments. If you paid out-of-pocket (and you have requested in writing that we not bill your health plan) in full for a specific item or service, you have the right to ask that your PHI with respect to that item or service not be disclosed to a health plan for purposes of payment or health care operations. We will honor that request unless it is required by law to do otherwise.
- The Right to Request This Notice by E-Mail. You have the right to get a copy of this notice by e-mail. Even if you have agreed to receive notice via e-mail, you also have the right to request a paper copy of this notice. To obtain a paper copy of this notice, please contact the Privacy Officer.

CHANGES TO THIS NOTICE

We reserve the right to change this notice and the revised or changed notice will be effective for information we already have about you as well as any information we receive in the future.

COMPLAINTS

If you believe your privacy rights have been violated, you may file a complaint with the Privacy Officer. All complaints must be in writing. You also may send a written complaint to the Secretary of the Department of Health and Human Services in Washington, D.C. within 180 days of an alleged violation of your rights. We will take no retaliatory action against you if you file a complaint about our privacy practices.

PERSON TO CONTACT FOR FURTHER INFORMATION OR ASSISTANCE

If you have any questions or need further assistance regarding this notice please contact:

Privacy Officer
C/o Post Acute Medical, LLC
1828 Good Hope Road, Suite 101
Enola, Pennsylvania 17025
HIPAAPrivacy@postacutecorporate.com
833-246-1088

EXHIBIT C

Terms of Use Policy

By accessing and using this website, you agree to these terms and conditions. PAM Health ("PAM Health") can change this agreement at any time. Any such modification will be effective immediately upon posting.

Intention / Use of Website

This website does not offer medical advice.

Website content -- including graphics, images, text, and all other content – is shared for reference and educational purposes only. Website content should not be interpreted by the user as personal medical advice.

PAM Health makes every attempt to make sure the information on this website is correct and consistent; however, it offers no guarantees. This website is not an attempt to practice medicine or provide specific medical advice, and it should not be used to make a diagnosis or to replace or negate a qualified medical provider's judgment.

Some information on the website is written by medical providers affiliated with the PAM Health system and its affiliates. Other information is from outside sources.

Medical Disclaimer

In case of a medical emergency, immediately call your doctor or 911. This website is not intended to to manage medical emergencies. For immediate, urgent medical needs, do not rely on electronic communications or communications through this website.

Medical Content

In case of a medical emergency, immediately call your doctor or 911. This website is not intended to manage medical emergencies. For immediate, urgent medical needs, do not rely on electronic communications or communications through this website.

Liability

Website visitors assume full responsibility for using the information on this site, and you understand and agree that PAM Health and its affiliates are not responsible or liable for any claim, loss or damage resulting from its use by you or any user.

External Links

To provide website visitors with additional information, PAM Health may have links to other websites. However, PAM Health has no control or authority over external linked websites. External pages and sites have separate terms of use. In addition, a link to an external website is not intended, nor should it be interpreted, as an endorsement of those products or services.

Copyright

Unless otherwise noted, all information on this website is copyrighted by PAM Health.

Use of this website constitutes your agreement to our Terms of Use policy.

You acknowledge and agree that all content and materials available on this Website are protected by copyrights, trademarks, service marks, patents, trade secrets, or other proprietary rights and laws. Except as expressly authorized by PAM Health, you agree not to sell, license, rent, modify, distribute, copy, reproduce, transmit, publicly display, publicly perform, publish, adapt, edit, or create derivative works from such materials or content.

Compliance/Privacy